Global Payphones

Taipei, Taiwan. This thing truly scares us

Photo by MC Telecom

Turku, Finland. Note the funky coin mechanism on the top and the extra long cord.

Photo by Chase Brown

Freeport, Bahamas. Amazing what a little color can do.

Photo by Pentastuy

Ch'ongju, South Korea. There's a lot going on here.

Photo by C. Jacques

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

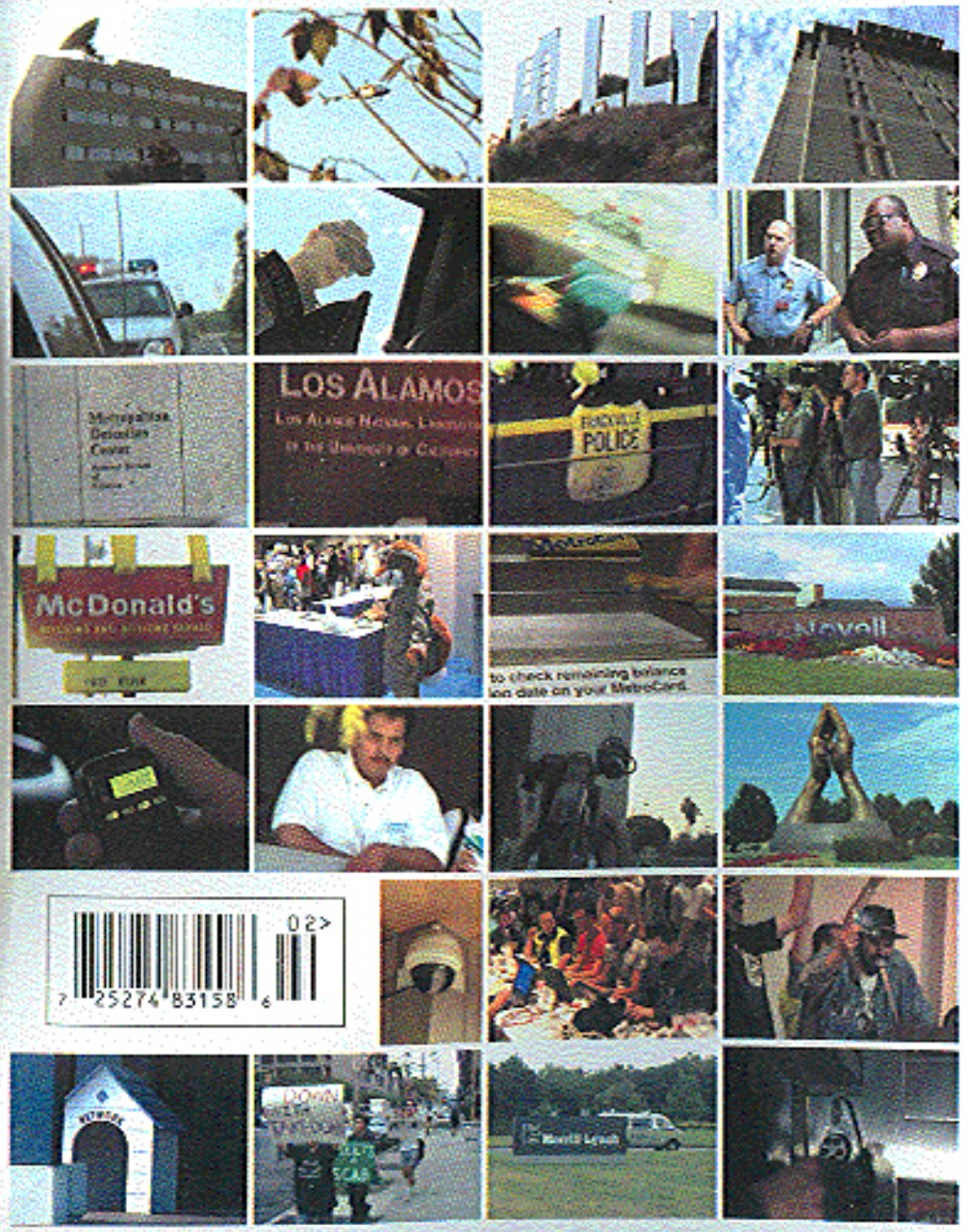
2600

The Hacker Quarterly

Volume Seventeen, Number Two

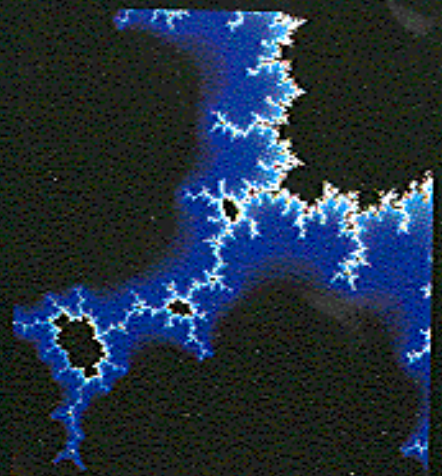
Summer 2000

$5.00 US, $7.15 CAN



FREEDOM DOWNTIME

HOPE 2000
HOtel PEnnsylvania
New York City
July 14th to July 16th, 2000



H2K

It's not too late!
(Well, it is if you read this after mid July.)
Keynote speaker: Jello Biafra
Premiere showing of our documentary
"Freedom Downtime"
Two tracks of speakers and panels plus
films and music around the clock!
See page 56 or www.h2k.net.

THE NEVERENDING FLOW

"Posting information about MPAA's anti-privacy operations and techniques will make that information easily available to those engaged in, or planning for, digital piracy of individual works." - MPAA's "Director of Anti-Piracy, Worldwide" Kenneth A. Jacobsen in a filing to the court to prevent the media and the public from learning what they are saying in pre-trial depositions. He really did say "anti-privacy operations" in his filing. Freudian slip? You decide.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
tankedUPqueer

Cover Design
Matt Protagonist, The Chopping Block Inc.

Office Manager
Tamprut

Writers: **Bernie S., Blisf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dortman, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Mift, Kevin Mitnick, The Prophet, David Ruderman, Serat, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmaster: **Macki**

Network Operations: **CSS**

Video Production: **Porkchop**

Broadcast Coordinators: **Juintz, Shiftlock, Absolute0, silicon, cnote, Anakin**

IRC Admins: autojack, ross

Inspirational Music: Evan Chen, The Protestants, Moby, Eels, Elliot Smith, The Wiseguys.

Shout Outs: A16, Royston Vasey.

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.*

POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate. Back issues available for 1984-1999 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631-474-2677**

MADNESS

While many are deeply distressed, who among us can say they're surprised at the unfolding events of this year? Anyone who can needs to start paying closer attention.

Corporate America has gone mad with litigation and its obsession with the net. Meanwhile, governments the world over are doing everything possible to close the Pandora's box of freedom the net has created. It's getting pretty ugly out there.

Our troubles are only a small part of the story. Sure, we've never faced this kind of corporate venom before. But when things like the Telecommunications Act of 1996, Digital Telephony, the Digital Millennium Copyright Act (DMCA), and "end-cybersquatting" bills win easy passage, it's inevitable. The Internet, once the shining beacon of free speech, cultural exchange, and open expression is fast becoming the exclusive property of big business and oppressive regimes. At least, this is how it appears in their minds. We cannot let our own perceptions be corrupted by this invalid premise.

How else would it be possible to claim that a piece of e-mail (the "ILOVEYOU virus") could cause $10 billion in damage and that, once again, hackers are responsible? How would it be possible to completely gloss over the fact that, once again, all of the problems were because of a gaping weakness in a program called Microsoft Outlook and that this is a lesson that should have been learned from the Melissa virus a year earlier? Very few in the hacker world have been affected by any of these demonstrations of stupidity and it's because we know not to blindly trust programs (particularly ones from Microsoft) when it comes to security issues. The corporate media misses this vital point and instead looks at hackers as the cause of the problem, when anybody in the world could have done this simply by sending e-mail.

The way the media covers things is only a small symptom of a problem that continues to get worse. Several years ago it would have been almost unheard of for a corporation to bully someone into submission on the net using nothing but its might. Today we seem to hear of a new case every day.

No doubt a lot of what's happening is bolstered by court developments such as those which are proceeding against us. And if we were to back down and agree that it was acceptable to deny people the right to know how technology works, a dangerous precedent would be set and then you would see a hundred more lawsuits filed for "offenses" ranging from writing source code to writing articles about source code.

It's safe to say that new developments in technology are scaring the corporate world to death. What milestones like Napster represent to them is a potential loss of the control they've held for so long. Whereas before, record companies (yes, most of the major ones are owned by the same corporations suing us under the DMCA) made the decision as to what music would become popular, now the potential exists for people to do this on their own and completely bypass the traditional means of distribution. There's little debate that this could erode some of the massive profits these companies currently enjoy. But it's far less clear that artists themselves would be adversely affected. Many, particularly those who aren't already in bed with the record companies, have come out in full support of Napster and the increased ability for the consumer to choose.

Naturally, the music industry has distorted the issues in this case in much the same way the motion picture industry has distorted the ones in ours. For one thing, all Napster does is point people to sites that have the music they're interested in. One could even consider that to be a service to anyone wanting to shut those sites down. Another issue is that the record companies seem to believe they have the right to make money every time someone hears a song they own. This is the same mentality that has made it illegal for Girl Scouts to sing "Happy Birthday" around a campfire. The truth is, they don't have this inalienable right to get paid each and every time someone plays their music. Unless we give it to them. The net is merely a new medium, the modern day equivalent of trading cassettes with friends. In fact, CD sales have been increasing over the past year. The record companies' reaction? They would have increased even more were it not for MP3s and things like Napster. Right. Eventually, they will lose this battle but not before wasting a lot of time and money trying to stifle the development of technology.

A wise man once wrote, "That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property."

That wise man was Thomas Jefferson.

We don't favor piracy in any way. People who sell CDs that they have burned are clearly making a profit off of someone else's work. But sharing

Continued on page 40

THE ART OF SYSTEM PROFILING

by Thuull

Opportunity Hacking is the process of finding a neato new exploit that you somehow manage to get compiled... so you scan the *entire* Internet looking for any system at random that just happens to have the hole that you know how to get into. Lame.

System Profiling is the act of picking out one system or network and saying to yourself, "I want in *that* system," then researching the system or network to learn what it does and how the system works.

System Profiling is not about finding a single hole in a system, accessing the system, and considering yourself done.

System Profiling is about learning all there is to know about the system in question... maybe it has holes, maybe not... but a successful system profile does not have to result in owning the system. Hacking is all about learning, right?

This article is for a specific target audience. It is not designed to be interesting for script kiddies. If you are a script kiddie, and are only here to be a part of something bigger than you are, skip this article.

Specifically, this is targeted at system administrators, security professionals, and non-malicious curious people interested in the security of complex, heterogeneous networks.

Target

For the purposes of this article, we are going to assume that your target company, "ABCorporation," is the secretive type. They don't want you playing around on their network. They have firewalls, they have both active and passive Anomaly ID Systems. (Note: Active IDS Systems are those such as ISS RealSecure, which sit on a network and look for known "attack patterns" in real time. Passive IDS Systems are those that take information passing through the network and store it in some database, for anomaly detection and/or data correlation at a later time). They have a trained staff of security professionals.

But, of course, this is what interests you about the ABCorporation....

Start your profiling simple. Use the services that they *intend* to make available to the public to glean whatever information you can.

Website

Surf their website. Many companies will make available on their web sites all kinds of interesting information about the people who work there, their computer systems, their business partnerships, etc., etc., etc. Use this information to your advantage.

They have e-mail addresses on there? Those *might* give you the username scheme that they use... worth a try. One of my favorites... do they list the names of their sysadmins? Some do. Tell me, how do sysadmins find new jobs these days? They post their resume on the Internet!

Do a couple of web searches on the sysadmin's names. Check out www.monsterjobs.com, www.dice.com, and www.computerjobs.com, as well as a slew of similar sites. See if you can find their resumes online. Maybe someone who works there now is attempting to jump ship.... If you do find one of these resumes, you can just about guarantee that you now know what kind of systems your target company is using. Is the guy(s) a CNE? Bet they use Novell.... MCSE? Well, Windows then... you get the idea.

Usenet

Any names that you get of employees off of web pages or other means, go out to dejanews and do a search on the names. You'd be surprised what you may find there. Or simply do a search at dejanews on "@ABCorporation". You'll see the posts of everyone with one of those e-mail addresses.

I once found a string that a firewall administrator at my target company had started... guy was having problems with his ipchains firewall and was looking for specific syntax advice. He had gotten frustrated in the string because he was getting disjointed responses. So he posted his entire list of chains and the exact syntax of every rule in every chain.

Whois

There are other sources of info too. Pull up a terminal. Start doing whois's: ABCorporation@arin.net, ABCorporation@whois.ripe.net, ABCorporation@whois.networksolutions.com, ABCorporation@whois.internic.net, you get the point.

You'll find that the different databases list different things about your company.

Most companies will have multiple blocks of IP addresses... some of these blocks will be portions of the network that used to belong to another company, perhaps a company that had been bought out, etc. But we'll get to that in a little bit.

There was a company that I targeted at one time that had seven different Class C address spaces, one of which was subleased from a local ISP. As all of the other blocks were through *major* Internet carriers, I checked out the Mom and Pop one.

Turns out a disgruntled division in the company, their distributed programming department, had been denied the use of ICQ through the corporate firewalls.

So, they went out to Mom and Pop ISP and got themselves their own ISDN line. But they didn't realize the need to put a firewall on it *and* the boxes they put on this ISDN line were all dual-nic'd windowsNT machines, default install. They also didn't realize that the Mom and Pop ISP had subregistered the IP block with ARIN, with their company name, so it showed up as one of the blocks belonging to that company with a simple "whois ABCorporation@arin.net".

Obviously, on the first nic, tied to a hub which was tied to their ISDN router, were the public, routable IP addresses. Guess what was on the other nic in those machines? Yup, that's right. 10.x.x.x IP addresses.

For any of you who don't know what I mean - they had these unprotected NT machines tied into their internal corporate network, i.e., on the company's "clean" side of the firewalls, fully accessible via routable IP addresses from the Internet. Basically, corporate security policy gone wrong.

Dig

Another way to find different "blocks" of IP addresses that belong to your target company is by utilizing the company's (or more preferably, their ISP's) domain name servers. Most will gladly hand the information right over to you. Try this:

dig @ABCorporation.com ns

This dig command gives you the name servers that service the target domain, in this case "ABCorporation." With the names of these name servers, you can attempt to conduct dns zone transfers of your target company. Let's say that the output from this dig command gives you three dns servers:

ns1-auth.sprintlink.net
ns1.ABCorporation.com
ns2.ABCorporation.com

Now, consider the output. You know that your target company has intrusion detection systems. So you want to attempt to gain information about the target company's network without the traffic crossing the IDS system. If you try to zone transfer from the dns servers at ABCorporation.com, your request will probably travel across the firewall, and hence probably across their IDS systems. However, ABCorporation is not going to have IDS systems physically located at their ISP. So:

dig @ns1-auth.sprintlink.net ABCorporation.com axfr

If ns1-auth at sprintlink allows zone transfers, you've just managed to get the complete zone of the machines, with IP addresses, at ABCorporation that are publicized via dns, *without* irritating the IDS system at the target company.

"So?" you ask. Consider this output from the above command (IP addresses have been changed to protect the innocent):

```
<snip>
track 1H IN A 201.195.10.142
clientop 1H IN CNAME www2
oh 1H IN NS ES1.ns
ES1.ns 1H IN A 10.30.1.78
oh 1H IN NS ecns2.nc
es2.ns 1H IN A 10.30.1.79
ns 1H IN A 201.194.241.2
prodftp 1H IN A 201.194.241.3
mail 1H IN CNAME corp
aur 1H IN CNAME spree.com.
inet 1H IN A 201.195.10.10
testftp 1H IN CNAME prodftp
ns2 1H IN A 201.194.241.6
ns1 1H IN A 168.4.1.65
auth02 1H IN A 168.4.1.82
products 1H IN A 209.119.113.161
corp 1H IN A 201.195.50.201
ftp1 1H IN CNAME prodftp
pdk 10M IN NS ns
<snip>
```

All kinds of cool information. Let's analyze. First, notice that there are six different routable Class C address spaces represented in just this one little <snip> of the axfr output (which is only about 13 percent of the total output). That gives you six different entire class C's which you can safely assume belong to the same company. Second, and this one is really cool, notice those 10.30.1 addresses? Those are non-routable on the Internet. The entire 10.x.x.x Class A is non-routable - "Reserved for Internal Use." Hello.

As it turns out in this case, ES1.ns and es2.ns are interfaces on the company's border routers, on the outside of their firewalls, and on the outside of their IDS's. So what, can't route to 'em, right? Sorta... these are the company's border routers, i.e., the same routers that connect the

company to their upstream service provider. That being the case, the routers must also have routable IP addresses. See line 11? "inet 1H IN A 201.195.10.10" That's another interface on the same router that holds ES1.ns. And it's telnetable. So, telnet into that router. In this case in particular, the username/password were ABCorporation/ABCorporation. From there, telnet to other 10.30.1.x IP addresses. What else was on the 10.30.1.x address space, you ask? Well, all of the firewalls had 10.30.1.x interfaces, as well as their CA Unicenter boxes (network discovery), as well as some of their internal routers. All of this was on the inside of the firewalls. Of note, you are going to need to find another machine on the inside that you can telnet to from here in order to do any real investigation. Right now, on this router, you cannot compile exploits, etc., as you are on a router. In this case, that CA Unicenter box I mentioned had telnet open with the same username/password as above. Bingo, Solaris 2.6 machine.

I found out later that they had done this because the nature of the company's remote access from home didn't allow them to access the border routers while dialed up to the internal network when they worked at home. So, they needed a way to connect to the border routers (which they could reach from the Internet), and from there into some of the internal network devices inside the firewalls. Another case of corporate security policy gone wrong. The policy had good intentions, but internal employees who were inconvenienced by these policies created a way around them. They had no idea what this meant to the security posture of the organization.

Business Partnerships

Okay, we already said that your target is paranoid. Let's assume at this point that none of the above vulnerabilities are available directly from the Internet. But, you do know that your target company has a close business partnership with a web-portal: XYZCompany, let's say. (You learned this from your website jaunt earlier.)

Well, typically, a company who has a tight business partnership with another company, depending on what the companies do for each other, will have special services allowed through their firewalls between them. They might even have a dedicated point to point or two between the two companies, sans firewalls.

Take a quick look at XYZCompany. Are they a Mom and Pop shop? Twenty employees? Internet presence? Bet they'll be a lot easier to get into than your final target. And, once there, you can enjoy relaxed restrictions into your target company... probably.

Corporate Acquisitions

Along these same lines, look for companies that have recently been bought/acquired by your target. In most large organizations, the process of buying another company is a long and tedious one, but the primary reason for technology companies to merge is so that they can use each others' technology. So one of the first things to happen is usually a change in firewall rules, or the establishment of an internal network link to the "new arm of the company."

However, a corporate merger is a political beast.

Company officers will normally be very careful about stepping on toes, especially since the guy who used to be the CEO of the bought company is now a VP in your target company and probably a little touchy. So the extension of corporate policy to the "new organization" usually takes a couple of months, or even years to be fully enforced. The same thing applies to the security policy.

Normally, the company that was bought is usually a lot less established than your target, so maybe they don't have a security department. Maybe their sysadmins are lazier - who knows?

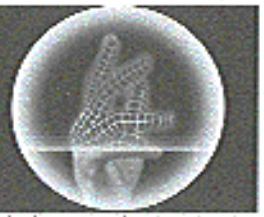
What does this mean to you? Quite simply, profile the recent acquisitions.

Perhaps you're picking up on a subtle theme here.

Sun Tzu, in "The Ancient Art of War" said, "Where you are weak, make your enemy think you are strong, where you are strong, make your enemy think you are weak. Attack your enemy in his weakest point with your strongest force. In this way you will be victorious." or something very similar....

In practical terms, you know they have firewalls, you know they have IDS systems, why bang your head on those protected avenues when you can probably find an avenue that's not protected at all?

A Brief Intro To Biometrics



by Cxi ~

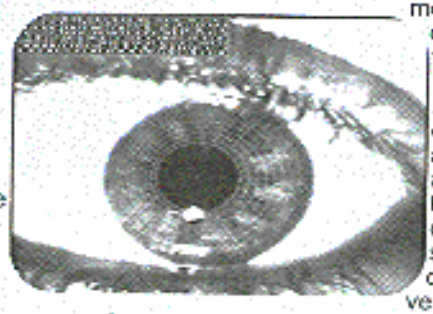
A new area of physical security that has become increasingly popular, and will become exponentially popular as its uses are more easily implemented and its need is more clearly seen, is Biometrics or Bio-access. Access to what? Biometrics is not just to be used in access to buildings or computers, but will soon be used for access to your bank account, your credit cards, or even to make a phone call. Biometric systems grant access based on personal identification, which is based on a preprogrammed pattern of recognition, providing not only identification but also verification. In order for this to work, we must keep in mind the theory that physiological traits are unique for everyone. I will give you a quick synopsis of what occurs when you use a biometric system.

The process for identification begins with a request for recognition by a person who submits certain biological information. This is then compared to an existing database. The speed of this process all depends on the size of the database, size of the usually large file, and processing speed of the computers. New compression technology is shrinking the file size of this "bio 411," allowing for a larger capacity to process large amounts of comparison data.

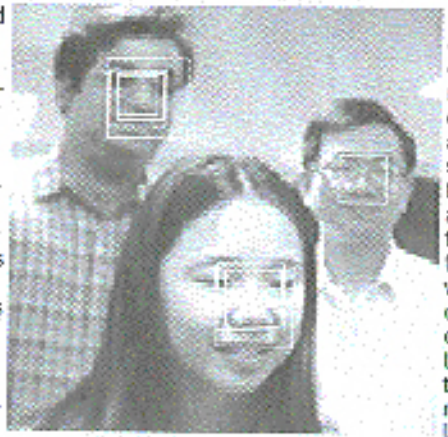
For the most part, biometrics requires contact with body parts. Because of the chances of disease transmission, video and laser scanning are being implemented in many applications to eliminate the need for anyone to touch anything. With the constant use of computers today, securing access and information is no longer a business matter, but something that people have to be concerned about in their private lives as well.

There are seven common biometric categories being used today. Fingerprint, hand geometry, retina scan, iris scan, facial geometry, voice verification, and signature verification are all considered a part of biometric security. Fingerprint analysis is the oldest and most commonly known form. But this has evolved from the old ink and paper system. Current systems take video images of the fingerprint and break it down into various components. The ridges on the fingerprint are converted into mathematical keys so that each fingerprint is really a series of mathematical equations. Also, the more fingers used for identification means a more accurate verification process. But, this also means doubling, tripling, or even quadrupling the storage size needed. Higher resolution of the systems allows for more of these equations, which in turn results in greater accuracy. Initial reading and storage can take anywhere from five to ten seconds and verification only about one or two seconds. Hand geometry is very similar to fingerprint systems and is actually just an extension of them. It creates mathematical equations usually based on the height, width, and length of the hand. This could lead to a possible problem with

very identical twins who have the same hand size. Retinal scans require the examination of the eye at a close range (about one to two inches). This is very intrusive and long and therefore has only been implemented in places with very high security requirements. An iris scan makes a mathematical map of the iris (area around the pupil). With an estimated 200 points within the iris, it is fairly easy to do so and can be very discriminating depending on how many points are processed. Since eye color is not the issue, black and white cameras (which translates to cheaper systems) can be used to capture the image, which will be stored and compared to a live scan during the next verification process. This is much more accurate than hand geometry because even members of the same family, including those very identical twins, will have different iris scans. Face geometry is the result of hand and finger recognition. It takes a video image and selects facial points in order to make a decision to grant access. The most common use determines the distance between two points on the face. Another use involves measuring heat spots with an infrared camera (which translates to more expensive systems). This avoids problems created by objects that may cover the face. Voice verification has also become increasingly popular. It analyzes voice pitch, speed, and pattern and forms it into a personal digital signature. Many systems have been made more accurate by requiring a standard word pattern to be used for reference identification and confirmation. This is also a system that avoids disease transmission because it requires absolutely no physical contact. Signature verification divides a person's signature characteristics into two parts: those that remain constant and those that change. This usually requires using an integrated writing tablet system and can be very costly.



There have also been many different implementations of these kinds of bio-access. Many require some form of card access that is verified by one of the previously described methods. This makes the verification process much quicker since the computer merely compares the live data to the data matching the owner of the card as opposed to searching the entire database for a match (or to not find a match). Future technology will use smart cards to hold the comparison data themselves and therefore eliminate the need for larger, quicker databases to store and process these large bio-information files. But can you just imagine what would happen if someone (and you *know* they will) figured out how to hack one of those smart cards? People would be able to create their own identities pretty easily and gain access to restricted places without much effort on their part, since the computer let them in. And computers never lie, kid (sorry... lame ass *Hackers* quotation. I know... but it had to be done). Also, compatibility is an issue. Many manufacturers of these systems use different protocols and therefore you can't have a "universal file" to be used on all security systems everywhere... yet. But obviously this is something the government (Department of Defense) would want and supports not only with words but also with funding supplied by the National Registry. With the possibility to keep every person's unique characteristics on file (not to mention what else would be possible) and maybe not even need to store the file on your own computer with the new smart cards, wouldn't you prefer to do this? A committee known as Bio-API has been formed to look into creating standards for the industry. Another standard developed by many industrial developers, the government, and even MIT is the Speaker Verification-API (SVAPI). There is a free software developer's kit online which I suggest you download if you're a Windoze person (95 and NT).



Biometrics itself is such an intrusive and invading procedure that many have said it needs its own form of security. However, as of yet there is no law or regulation governing the sale or transfer of biometric information that is legally acquired. This means that if you apply for a job and are required to submit to a biometric scan, the controlling agency provides absolutely no protection for your private information. There is a pending California bill, AB50, which is attempting to stop the copying of biometric information. Another issue for concern is the efficiency of such systems. Are they really needed? Are people going to stop using ATM's or banks because they can't stand to wait for that damn iris scan only to learn that they can't get their money because of some system bug? Well, the National Biometrics Test Center has developed testing standards for evaluating the performance of biometric access equipment, previously only performed by the manufacturers. The best chance for standardization has come from the National Computer Security Association which has created a certification program for systems and system components such as scanners that will set error rates based on a standardized testing method.

Now, we can look at this new technology any way we choose. If it's left in the hands of the private and business sectors, and used in ways which doesn't discriminate or eliminate people's options for doing things, this can be a great thing and an added level of security for people in their homes, and for businesses fearing corporate espionage or whatever paranoia they may have. However, if placed in the hands of the government, we could be giving them one more power that would enable them to control and monitor our lives. Depending on where these systems are made, the government could be able to watch when we come and go from our houses, log on to our computers, take money from an ATM, or even see what pay-per-view movies we buy. That my friends, is a very scary thought and something I hope I never have to think of as a reality.

Here are some biometrics manufacturers if you would like some more information:

HID
Biometrics2000.com
Identix

For more information about biometrics check out these websites:

Iris-scan.com
biometrics.cse.msu.edu
www.dogpile.com - find stuff yourself!

Shouts: ASleep, glock, minus, LordViram, and the rest of the ct2600 crew!

Fun With TDOC

by Anonymous

The Tennessee Department of Correction (TDOC) has "upgraded" their little piece of the State's network. MIS (Management Information Systems), the people responsible for the piece of crap called TOMIS, was given the task. TOMIS runs under UNIX as a clumsy interface with infuriatingly cryptic menu names and a pathetic online help menu.

As of November 1999, TOMIS users said goodbye to their old Memorex Telex terminals and received MTX 1683 terminals. This is because MIS and "The Powers That Be" didn't like the idea of having several PC's connected to TOMIS for the paperpushers to do their memos and stuff on. Their paranoia was well placed because the PC I used was equipped with Q BASIC and the client app for connecting to TOMIS (grin). The prison staff are under trained and barely computer literate. Most staff had dumb terminals, so PC security has been largely overlooked.

Is the system "secure" now? MIS laid a shitload of fiber, bought hundreds of MTX terminals (diskless), 15" color monitors, and printers. Now TDOC staff have access to the State's NT server! Of course, they didn't do any real training and the staff are still clueless about how to do anything above the simplest tasks. MIS didn't want to go through all the trouble of putting all the TOMIS stuff on the NT server, so you can either log onto TOMIS or the NT (but not both). The NT provides access to MS Word, Excel, email, etc. I didn't see anything all that exciting on it, but it's worth exploring because of all the subnets attached to it.

Due to the poor training, I was lucky enough to have the opportunity to spend several hours on the TOMIS and NT "helping" teach the staff I work for. What incarcerated hacker would pass that kind of chance up? After a short time I realized that one of the little MIS idiots forgot to set a configuration password on one of the terminals. Under the watchful eye of clueless staff members, I was able to view and change anything I wanted. Anyway, here's a little info for anyone who's interested in checking out one of the most pathetic systems I've ever seen.

NT Server

Domain Name: state.tn.us
DNS Server: 170.142.82.150
Default Gateway: 170.142.48.129

TOMIS (UNIX)

Domain Name: tn3270.state.tn.us
Port: 23

Warning: TOMIS only runs batch processes (called "conversations" or "requestable reports") and any interactive process will stand out.

Login Proceedure

1. Type IMS2 under State Map (hit enter).
2. Type BI"NUMBER" (replace "NUMBER" with a valid user ID).
3. Tab down to Password field and enter password.
4. Type in the answer to the two personal questions (there are two of them from a list of twenty).
5. You are now at the Main Menu. Move your cursor to the lower left hand corner of the screen next to Function and type in the conversation you want from the following list.

LCD2: visitor status
LCD3: staff assignments
LCD4: institution travel
LCDA: standards
LCDB: fee types
LCDC: treatment programs
LCDD: criminal justice person
LCDE: staff
LCDF: plan of service
LCDG: contact notes
LCDH: travel
LCDI: offender fee inquiry
LCDJ: revocation warrants
LCDK: transfer in request
LCDN: family/contacts
LCDQ: fee payments
LCDR: fee exemption
LCDU: offender fees
LCDV: offender receipts
LCDW: work site assignment
LCDX: work site referral
LCDY: work site report
LCDZ: work site application
LCLA: offender attributes
LCLB: offender aliases
LCLC: offender employment
LCLD: offender treatment
LCLE: offender education
LCLF: offender findings
LCLG: offender orientation
LCLH: inst transfer request
LCLJ: PSI referrals
LCLK: PSI text
LCLL: offender debts and assets
LCLM: PSI victims
LCLN: classification
LCLP: classification test results
LCLR: criminal history
LCLS: assignments due
LCLT: CAF weights
LCLV: CAF score
LCMA: commissary item
LCMB: commissary purchase
LHSB: accident
LHSE: health assessment
LHST: limited activity notice
LHSV: health history
LIBA: incompatibles
LIBD: segregation
LIBE: future disciplinary hearing
LIBF: grievance
LIBJ: incidents
LIBK: disciplinary
LIBL: disciplinary decision
LIBM: board/committee members
LIBN: offender property
LIBO: offender property arrival
LIBP: offender claim
LIBQ: cell search request
LIBR: cell search results
LIBS: drug audit results
LIBT: property audit findings
LIMC: RQST cell/bed assignment
LIMD: arrival/departure
LIMF offender cell change
LIMG: chain schedule
LIMH: dead offender
LIMJ: escape transfer
LIMK: escape
LIMM: visitor history
LIMN: current visitors
LIMQ: count room
LIMR: pop counts
LIMS: site
LIMT: admit request
LIMV: non-rider
LIMW: schedules
LJEA: offender pay
LJEB: education test results
LJEC: program notes
LJED: job/class assignment
LJEE: job/class termination
LJEF: job audit
LJEG: work permit
LJEH: job/class register
LJEJ: register placement
LJEK: job set up
LJEL: position request
LJEM: job position ID
LJEN: offender attendance
LJEP: pay policy
LJER: class section
LJES: special education referral
LJET: job/class inquiry
LJEV: class set up
LOEB: diet order
LOEC: drug order
LOED: radiology order
LOEE: laboratory order
LOEJ: radiology results
LOEK: laboratory results
LOEL: services provided
LPDA: board action
LPDB: parole/committee recommendation
LPDD: interested party/comments
LPDE: parole predictor
LPDF: proposed plan
LPDG: SAIU findings
LPDH: probation petitions filed
LPDJ: hearing subpoena request
LPDL: ISC requesting courtesy
LPDM: other state recommendation
LPDN: parole staff action
LPDP: eligibility docket
LSSA: TOMIS user ID
LSSB: security alert
LSSC: access revocation
LSSD: security conversations accessed
LSTA: dead/delinquent/street time
LSTB: offender credits
LSTF: offense statutes
LSTJ: judgment order
LSTM: credit law waiver
LSTP: ISC sentences
LSTQ: Tennessee sentences
LSTR: sentence actions
LSTS: detainer
LSTT: diversion
LSTV: SMS offender credits
LSWA: e-mail
LSWB: report request
LSWC: report set up
LSWD: TOMIS ID add
LSWE: phonetic compare
LSWF: user procedures
LSWG: forms maintenance painter
LSWH: restore offender
LSWK: terminal printer
LSWL: TOMIS ID maintenance
LSWN: name search compare
LTFB: trust fund organization

LTFC: payroll release request
LTFE: trust fund transactions
LTFH: trust fund obligations
If you choose a conversation that requires a Site ID, here are a few to get you started:
BPCO: Board of Parole Central Office
CENT: TDOC Central Probation Office
CNRC: Central Records
DCCO: TDOC Central Office
CNV: Conversion
EIC: Escape Information Center

Need Help Using TOMIS?

The TOMIS Hotline (aka System Development Services) can be reached between 8:00 a.m. and 4:30 p.m, Central Time Monday thru Friday. If you don't like dealing with personnel who might be sitting at a terminal trying to figure out who you are, then just call their on-call people! They aren't at a terminal, but are very willing to give out info to anyone who has their pager number. Call 1-800-841-7243 between 10:00 p.m. and 12:00 a.m., Monday through Friday. On Saturday and Sunday it's 7:00 a.m. to 4:00 p.m. Another interesting place to look for information is the Data Center. TOMIS users call this number when reporting equipment malfunctions.

System Development Services
(615) 741-1000
The Data Center (615) 741-1001

If you're reading this article and thinking, "Hey, I could hack TOMIS and change prisoner release dates and they'll let them out!" you're dead wrong. Central Records checks each inmate's paper file before releasing them. Hacking isn't about short circuiting "justice" anyway, is it?

Strange Abuses For Your Home Phone

by Static

static@mentalwaste.8m.com

There are quite a lot of rather strange phones on the market right now. One of them is the Conairphone model: HAC SWS260. This little bugger consists of an almost bite-sized control and a 1/8 inch input/output jack that the headset (the part through which we speak and listen... please stop me if I'm getting too technical here) connects to. The little 1/8 inch headphone-plug sized jack is what makes this article worth printing. With the proper wires or patch cords and plug adapters, we can do all kinds of fun shit. Any piece of audio equipment can be used in conjunction with this phone since the input and output all come from the little jack. Some of the things we can do are: record any phone conversation of interest without notifying the party/parties on the line, patch peoples' most intimate conversations into PA systems, and generally put any noise we wish directly into the phone. While recording conversations over the phone is nothing terribly exciting or new, this is a somewhat newer and lazy way to go about it. Hell, if I want to talk to somebody and record the conversation, I just rig a microphone into a karaoke machine and plug the phone into the machine and vice versa. The new thing however is this inane little possibility: Musical performance for multiple people over the phone from the privacy of anywhere, as you can plug instruments into the phone. I'd very much like to be the first musician to ever do something like this (if anyone would possibly be interested in this venture, do drop me a line sometime. (I play Industrial/EBM/Darkwave/Electronica/Ambient/Whatever.) All of the wires and adapters can either be bought at the store we've all come to know and love/hate as Radio Shack, or your local music shop. Also, any phone with the aforementioned 1/8 inch input/output jacks is capable of this nonsense in case you don't feel like gravedigging all over to find the phone I use for this. And finally, there is a plethora of strange things one can attempt via phone with this method that I haven't or never will bother to think of... so I leave it to the rest of you out there to play with the options and attempt really oddball things. If anyone has any ideas about things to do, I'd sure as hell like to hear them.

More Advantages of AllAdvantage

by KireC

The article written about AllAdvantage in the Spring 2000 issue of 2600 caused me to look into the program for myself, in normal, hex, and reverse compile mode. They pay 50 cents per hour of your surfing (only if the browser is highlighted - this is unfair because most people multitask while using the browser and don't get credited) for up to 10 or 25 hours per month. You get 10 cents per hour of a referral's surfing time, but you can only get paid for the same amount you have surfed (i.e., if you have surfed 10 hours and they have surfed 15, you can only get paid for 10 of theirs). It's a fine deal, but would be much better if it counted time when other applications were highlighted, not just the browser. My goal in examining the program was to shut the ads off, as well as the whole bar, and still get paid. I used the green LED to test this, as well as checking my account status daily. Green LED means you're being paid, red means you aren't.

You do have the ability to turn off AllAdvantage ads, but not the whole box. The program needs Internet Explorer or Netscape installed in order to run, so it is dependent on those programs. The easiest way to stop the flashy graphics is to go into your browser options and turn graphics off. (MSIE is under the "Advanced" tab, in Multimedia. Uncheck "Show Pictures".) Before using the program, you can modify "starlup.gif" to be whatever you want it to be. The viewbar will force the image to fit, so image size doesn't matter. You can also change "startup.html" to change what it starts automatically. Whenever I start the viewbar, I look at 2600.

You are free to alter any of the html files in AllAdvantage's directory. However you should write-protect all files that you alter and backup the originals. After you start the program, it will create a few different web pages in its installation directory: "motd.html" and "ad.html" which will be deleted when you quit the program. While running the bar, edit those two web pages, and delete everything in between the two <noframe> </noframe> tags, save, and then write-protect your altered files. Next time you load the viewbar, you will see your own pages instead of the ads. Certain alterations cause the viewbar and/or whole system to crash. If this happens, hover your mouse over the AllAdvantage icon in systray (this will get rid of the AllAdvantage icon) and then lower your screen resolution, and say, No you do not like it and want it changed back. Your screen is now redrawn correctly.

Another way to just disable the ads and keep the viewbar open involves a hex editor with code access, like HIEW. There is html code inside of "viewbar.exe" that should be altered. Find the first occurrence of the ASCII "html" and that's what creates "ad.html" which shows us the ads. First occurrence is on line 004351f0. Don't alter the hex here, alter the code itself. Change lines 004351f0 to 004351f2 to noop commands, hex code 90. If you change the next lines, you won't get paid because they control the LED. The viewbar is then only loading the page "motd.html" and won't show you ads (it performs NO_Operation upon loading "ad.html"). I couldn't figure out how to shut the whole bar down, but these fixes will turn the ads off. If anyone knows how to turn the whole bar off, that would be helpful. Anyone interested in continuing this project should note that the program appears to have been written with Visual C++ because it uses an MFC (Microsoft Foundation Class).

As far as I know, AllAdvantage can't detect these, but they will probably start soon. They'll probably fix these bugs quickly and might cancel your account if you use this. That's why you backup the original files; reset everything when you download the new viewbar, it will probably check for some of these fixes.

Even if you do shut the ads off, you still need to actively surf (either in person or with a program). The point of this was just to see if it could be done. The best way for AllAdvantage to detect these is for them to check the user's actions based on repetitiveness and randomness. I don't condone turning their ads off and cheating them, nor do I condone their act of only crediting your account if your browser is highlighted. You are the only one responsible for any action taken with this information.

OVER THE VERIZON?

We counted 706 domains registered by Verizon, the new massive company formed by the merger between Bell Atlantic and GTE, including such classics as verizon-wireless blows.com and verizonshits.org. They seem to think that if they take all of the nasty words, nobody will be able to put up a site they don't like. When we found that they beat us to verizonsucks.com, we registered verizonREALLYsucks.com. That didn't go over well at the corporate office. They sent us a threatening letter and demanded that we turn it over to them or else. Apparently they feel that criticizing corporations on the net is now illegal. Since we made this public, many new sites have been registered by individuals with all kinds of nasty descriptions of Verizon (use your imagination). We grabbed verizonshouldspendmoretimefixingitsnetworkandlessmoneyonlawyers.com (yes, we believe it's the longest domain name possible). While we await the next threat, here's an entertaining list of all the Verizon sites we've uncovered. Remember, they spent 70 bucks on EACH of these!

DIRECTVVERIZON.COM EVERIZON.COM EVERIZON.NET EVERIZON.ORG GOVERIZON.COM GOVERIZON.NET GOVERIZON.ORG GOVERIZONCELLULAR.COM GOVERIZONCELLULAR.NET GOVERIZONCELLULAR.ORG GOVERIZONMOBILE.COM GOVERIZONMOBILE.NET GOVERIZONMOBILE.ORG GOVERIZONPCS.COM GOVERIZONPCS.NET GOVERIZONPCS.ORG GOVERIZONWIRELESS.COM GOVERIZONWIRELESS.NET GOVERIZONWIRELESS.ORG [illegible]

[illegible]

Securing ASP: A deeper cut

by AgentK
kent@tegels.org

In issue 17:1, Guinsu provided a primer on securing ASP-driven database-centric web sites. If you have not read that, it is worth doing now. In this article, I am going to expand on some of the issues Guinsu glossed over and discuss some alternatives. Not that I am going to provide the end-all, do-all. If you want that, read Richard Harrison's excellent book *ASP/MTS/ADSI Web Security* (1999, Prentice Hall PTR).

SSL is Only Part of the Solution

One principal of modern information security is not to make your security undefeatable, but rather to make it so costly (in terms of time, computing, and other factors) as to deter all but the most determined. Another principal is that the more you know about the parities in a transaction, the more trust you can have. These principals manifest themselves as encryption and authentication. Secure Socket Layer (SSL) is the current method of choice for encryption. For good reason - st current levels breaking 128-bit based encryption would require incredible luck or barely imaginable computer power.

Defeating authentication is a different matter. First, I recommend that you do everything you can to create "real" user accounts for secured site users. By this I mean populate an ADS or NTDS structure with accounts. Then add these accounts to groups. Finally, use NTFS ACLs to "lock down" the content and scripts to those groups.

Why not just store user accounts and password in, say, SQL tables? Two reasons: Well-secured directory services tend to query and respond faster than comparable SQL structures. And directory services tend to backup and recover quicker and better in the event of disaster than RDBMS services.

Keep in mind that IUsers will always use "password" (or something equally as inane) for their password. The weaker the password, the less you should trust it. What makes for good passwords? As a starter, I prefer:

At least eight characters, six of which can be from the English alphabet excluding vowels.

At least two of which must be digits (0-9).

At least one must be one of !, $, ^, or *.

No more than three of the characters in the password can be found in the User ID.

Logging users in can be an issue. Unless you know that your clients are using Windows and IE exclusively (a pity, but it happens), you're probably going to have to rely on the so-called "basic authentication." The level of password encryption here is, essentially, meaningless. So, if you are going to have to do it, at lesst require that a secured channel (e.g., an https session) has been started first. Then redirect to an ACL protected file set.

If you are going to have a secure site, SSL is certainly worth its weight in molybdenum. But so is - if you cannot use some other authentication technique - requiring strong passwords. Using Directory Services can be faster and more failure resilient. The best affect is achieved by combining the three.

Understand Your Environment

What I mean by this is that you need to understand how to secure your physical platform, how IIS works, and what can go wrong. Lets start at the hardware level.

A Good Foundation:

The most basic thing you "must" have for a security environment is a firewall. In my opinion, Microsoft Proxy Server is not good enough in and of itself to fill this bill. There's certainly nothing wrong with building a Solaris, Linux, or BSD firewall on an NT network, either. In fact, it can offer some advantages. Next, consider putting your Internet machines in a network that is otherwise detached from your internal network. Yes, it would be nice if all the system were "completely integrated" in some respects. Since you'll have to be willing to accept degraded security for your web platform, do you really want to risk everything on it?

One trick I've used is to use private networks with networks. For example, suppose you have three IIS servers with an exposed, registered IP address and you need an SQL server. There's very little reason to use an exposed, registered IP address for that. If you can use IPX/SPX, you could just add an extra NIC to each web server and to the SQL server, bind IPX/SPX to those. Thus web servers can talk free to the SQL server, but you eliminated some risks by not exposing the SQL server to IP-based attacks. If IPX/SPX is not an option, use private and not normally routed (10, 172.16 and 192.168) IP addresses to connect machines.

By the way, never put both IIS and SQL on the box if at all possible. You're just begging for both performance and security issues by doing this. NICs and hubs are cheap. Lost orders and leaked client information may not be.

The ASP Object Model

ASP is really nothing more than an application that runs inside the ASP process. In some respects, ASP is nothing more than a script interpreter. What is different about ASP is that it also retains state by the use of application and session objects on the server and response and request objects formed from the HTTP transactions. I could go on and on about this, but prefer not to. Get a copy of *ASP 3.0 Programmer's Reference* by Alex Homer (et al) (2000, Wrox Press) for the nitty-gritty.

Guinsu discussed the session object at length. Most of what he said was accurate. To overcome some of these issues, I recommend that all you store in session is one or two things: some unique key to represent the user (or user-session) and a reference to an MTS object that contains your data. This gets a bit complicated of course, but really helps both performance and security.

One thing that I would point out is that cookies are becoming more universally accepted but if your clients refuse them, you can use server-side persistence instead. Basically, this works as long as you can safely assume that your client will have a fixed IP address (or certificate serial number) for the duration of their visit to your site. You could then devise some data store using this as the key.

Something I felt did not get well explained is that ASP uses COM (and COM+) to pass scripts off to an interpreter. Thus, as long as the programming language you choose to use supports COM, you can use it within ASP. I prefer PerlScript, from ActiveState's ActivePerl. For what it's worth, Perl is not PERL.

What Can Go Wrong?

Like any system, power outages, theft, fire, and other common perils must be considered. But some Microsoft procedures and products can yield unannounced problems. A key one to consider is FrontPage and the FrontPage Server Extensions (FPSE). There are others, of course.

Ask any level headed SysAdmin about FPSEs and if you don't get a "bitter beer face," you'd better disable their account quickly (or at least make them recite "Security Considerations" from the "FPSE Resource Kit" three times, out loud, and in their underwear before the CEO and CIO). Remember that FrontPage was originally designed to make Web publishing easy. It overachieved. Part of the simplicity of FrontPage is that it managed the marshaling of files to and from Web servers transparently. When installed on default NTFS or FAT parti-

tions, anybody with FrontPage can access and edit files too easily. They can even upload harmful scripts and executable files. This is obviously *not* a good thing. Even more insidious, since FPSE are programs, they are susceptible to class attacks like buffer overflows. I do not know that "Netscape engineers are weenies" any more than Microsoft developers are a little too willing to compromise good security for ease of use.

Yet, you can actually tame these parasites - it just takes a little work. When installing on Windows systems, make sure that you put your \inetpub\ root only on an NTFS partition. Make absolutely sure to completely remove the "everyone" group from the ACLs for the partition or path before you install IIS (or as soon as you possibly can thereafter). *Do not*, however, deny "everybody," as nobody, not even the Administrators, will be able to access those directories. For good measure, I also turn on most of the auditing features for this path - just to see what people are doing. Installing the most current version of the Microsoft Data Access Components (MDAC) is also a prudent thing to do before installing IIS on NT4.

Next, make sure you have the most current version of the extensions installed for your platform. The ones that ship "Option Pak 4" and on the FP98 media aren't. Install these immediately after you get the IIS service installed and well before you connect the machine to an Internet pipe. Then run the FPSE administration program and run the "check and fix procedure." This will give you the option of "tightening security" which you should do as soon as possible. And, as a matter of practice, install every service pack and hot fix appropriate thereafter.

Something that's getting a lot of play as I write this are "Denial of Service Attacks." DoSA's are not hacking and you're not "l33t" because you can do them as far as I'm concerned. On the other hand, if you aren't designing your Web apps considering that somebody will pound it just to see how much abuse it can take, you are not doing yourself any favors either. If you create a bunch of objects during "session_onstart", even the "Human Ping of Death" could knock out easily. Rule of thumb #1: Create session objects sparingly, if at all. Rule of thumb #2: Expire objects as quickly and explicitly as possible. A sluggish server is almost always better than a dead one.

A small but dark cloud for you Windows2000 folks: Watch out for WebDAV. WebDAV (the Web Distributed and Versioning Protocol) extends HTTP's command set to allow FPSE like functions (and therefore, weaknesses) without FPSE muddling the picture. With WebDAV and enough access rights, folks can open, edit, and save virtually any file they have access to remotely. Again, taking great pains to edit your ACLs can impede the abuse of WebDAV.

There are a couple of other components to keep an eye on too. One of these is the FileSystem Object and its ability to read and write files on the server (see Chuck Newman's "Sharing Too Much" at www.webtechniques.com/archives/2000/04/newman/. Also, be very careful with any object-code library that lets users put files to server (SA-FileUp and ASPUpload). You're just asking for a trojan horse if you make those too easy to find and use.

Sleeping Well At Night

So, with all of these threats, gotchas, and gremlins in the ASP environment, can you sleep well at night, assuming that your web servers are safe? Taking the steps outlined herein can help, but the best you can hope for is that you've made it tough enough to break your site that the sHackers will go elsewhere for fun. The keys to a good night's slumber are: using strong encryption and authentication; understanding and hardening your environment and keeping abreast of, and reacting quickly to, what can go wrong.

Jello Biafra: Hacker Ambassador

by princessopensource

Jello Biafra, former front man for the Dead Kennedys, social activist, and keynote speaker for H2K, has never built a red box or hacked a PBX system. His "eleetness," however, is undeniable.

In a 1997 interview with the online magazine *Bad Subjects*, Biafra voiced his support of the Internet, along with the need for it to remain uncensored. His commitment to free speech in all forms of media comes with personal experience. In 1986, around the same time *2600* was celebrating its second birthday, police raided Biafra's home, searching for a poster of rotting genitals by artist H.R. Giger, copies of which the Dead Kennedys included in their album, *Frankenchrist*. Biafra was charged with "distributing harmful matter to a minor," but the case was later dismissed. Biafra has since become one of music's most ardent supporters of free speech, and is a vocal member of the organization, "Rock Out Censorship."

Along with his praise of the Internet, however, Biafra also had a few warnings about its dangerous potential for misinformation. He cautioned against allowing all the information the net bombards us with to numb our minds, as well as not being sucked into the belief that everything posted on a website is true. These words of advice are consistent with the hacker ethic by which many of us choose to live. Along with the adage, "Knowledge is power," comes the responsibility and desire to search for the truth and weed it out from the bullshit.

Jello Biafra is right on target with his warning about the sense-numbing experience an avalanche of multimedia can cause. If we do not take a stand against Internet censorship, the net could become just another outlet for the mass media to force-feed us a one-sided version of the "news." With increasing litigation over copyrighted domain names and software, a frightening future of the Web as a silicon-based equivalent of network television and Top 40 radio may not be as far off as we think.

Hackers need Biafra for his music and his mind. We need albums like *Frankenchrist* to remind us what can happen if we idly sit by and watch groups like the MPAA and RIAA take away our rights to create and use code and share music we enjoy with others. We end up like people the Dead Kennedys mocked in songs like, "The Stars and Stripes of Corruption." "The blind Me-Generation/Doesn't care if life's a lie/So easily used, so proud to enforce..." Biafra's post-Dead Kennedys activism and formation of his own record label, Alternative Tentacles, serve to illustrate that we must remain steadfast in our ideology. A corporate job in systems administration does not mean we should forsake our love for figuring out the "how's" and "why's" of the ways things work, and we need to ensure that the government does not eradicate our means to do so.

Jello Biafra's presence at H2K is sure to send a powerful message to both hackers and non-hackers alike - information does not just want to be free, it *needs* to be that way.

Hacking the Three Holed Payphone

by Munzenfernsprechermann

Once upon a time there were no computers to decipher, no electronic voice mail systems, no cable TV, and no Internet. There was one giant phone company and they built, owned, and operated all the payphones. These payphones were standardized. They came in one color (black) and in one basic style (see photo). Think about it. For almost forty years, phone hackers in the US and Canada were all tampering with the same piece of equipment. Over time, unauthorized people gleaned a substantial body of information on the mechanics and manipulation of these phones.

Although most of this information is now arcane, it may be of interest to present day phone phreaks or veterans who want to reminisce. The basic characteristic of this unit was the three different sized holes on top for inserting nickels, dimes, or quarters. Each coin generated a specific sound when dropped into the slot. A single ding for a nickel, a double ding for a dime, and a hearty gong for a quarter. Through these audible chimes, the operator could "hear" how much money had been deposited. These phones were invariably rotary dial, although some were retrofitted to tone dialing in later years. There was usually a coin return plunger in the upper right (missing in this photo) and a return slot or hopper on the lower left. The body of the phone was divided into two separate locked compartments. The upper part was accessible to repair personnel and relatively insecure. The bottom section was heavy steel and held the coin box. It required a separate key. The handset was connected with an unarmored cord and hung in a cradle on the left, which activated the unit when it was lifted. The whole thing was mounted on a cast metal plate that held the phone securely and sealed off the back and sides.

The basic game was to try and get a free or cut-rate phone call out of this ubiquitous black beast. Strategies consisted of various coin manipulations, messing with the wiring, or befuddling the operator (software?) to achieve this goal. A free long distance call was far more difficult and prestigious than a local one.

Coin Hacks

These phones required a coin to activate the dial tone. For the most part, you needed a dime or two nickels just to see if the phone was working. This characteristic led to beaucoup lost coins if a phone was out of order. Lost money was a common occurrence and undoubtedly began the adversarial relationship between the phoning public and the public phone. The least finessed method to get a dial tone was to use a slug to simulate the nickel or dime. Various foreign coins worked flawlessly, my personal favorite being the Trinidadian penny. Drop one in: ding ding, hummmmmm, you were good to go. Aside from genuine slugs made in high school metal shop, a favorite was the #10 large pattern brass washer. Available by the pound, they were the perfect width and diameter of a dime, but usually required a little tape over the hole or some spot to slow them down. They were not reliable enough for a long distance call (please deposit nine washers) but would usually generate a dial tone by the third try.

A rather elegant coin trick involved a nickel and some excellent timing. You dropped a nickel in the slot and if you slammed the coin return plunger at just the right time, you got your double ding and a dial tone. Of course, it was only a 50 percent discount and it hurt like hell, but it was handy if you were short on change. There were people who claimed they could use a coin on a string and pull it out but this was a myth since diameter, magnetic characteristics, and rolling weight were key in getting a coin accepted.

Hardware Hacks

Although not quite the fortress of solitude, this basic phone was fairly well guarded. The handset was unscrewable which was a boon to vandals but yielded little hacking opportunity. On certain models you could place a wire (paper clip, bobby pin, etc.) through the mouthpiece and then ground the other end to a conductive part (usually the coin return) of the phone. If done properly, it yielded a dial tone. I'd like to know how somebody stumbled across that one. Another similar stunt was to edge a piece of gum wrapper foil under the back right seam and slide it slowly up and down until you shorted out some essential wires, yielding a dial tone. I do recall getting a rather nasty shock while performing this maneuver on a rainy day.

A great deal of effort went into securing the phone itself but the wiring was often exposed. I believe it was a three pair line, but I don't know how many wires were essential. One pair carried a fairly high voltage to operate a coin drop solenoid in the bottom of the phone. Your cash was held in limbo above the coinbox. If your call was completed the money was dumped into the box or diverted to the coin return if the call was incomplete. I once witnessed a lineman shorting two posts at the junction box and yielding a load of change from a clogged chute. He told me he was often sent out to repair a phone that simply had a full coinbox. He also said the company security guys sometimes planted UV dyed coins in the upper end of the phone to try and catch their repair personnel stealing. I was never able to repeat his performance and yet I once again got a memorable electric shock for my efforts.

Some talented folks were able to momentarily short two of the wires to get a free local call. A bar in my neighborhood had a doorbell rigged to the line for that purpose. They maintained a Bell System employee who hung out there had installed it. It was rumored you could achieve the same effect by piercing the insulation with a pin.

The phones were hardened against attack, but they were often easily pried from their moorings. If one was stolen, however, it took a serious effort to get it open, which discouraged your average impatient thief. People were known to clog the coin return and return later to snatch it and reap their reward. This led to the retrofit of a coin return hopper (see photo) that was not so readily plugged up.

The blue and red boxes opened up a world of possibilities for payphone aficionados. There was a much simpler device that predates them and was pretty good at yielding a free connection for the caller. Sometimes referred to as the "brown box," it was a capacitor/resistor combination placed across the receiving end phone line. By absorbing the voltage surge when the phone was answered, the payphone believed the connection was never completed and returned the money when you hung up. Not as facile as a tone box, it was still a cool trick if you were calling someone with one of these devices. A phone installer found one in my house and he just confiscated it, along with half a dozen extension phones that were stamped "Property of the Bell System." Never heard another thing about it.

Software Hacks

Technically, these old electromechanical devices ran without software, but there were some decidedly non-hardware methods to outsmarting the payphone system. The most obvious was simply calling the operator and telling them the phone ate your dime. Sometimes they would mail you a dime but more often than not they'd put through a local call for free. For long distance calls, the operator would come on the line and ask you to deposit the cost of the first three minutes. By adding up the bongs and dings s/he would verify you entered the correct amount. If there was a dispute, they would simply return the change and have you reenter it. Some enterprising soul recorded these sounds and played them back but was foiled when the recorder deposited too much money. The operator activated the return solenoid, but when there was no handy recording of coins spilling into the return slot, the ploy was ruined.

Long distance calls were easily made with bogus or real credit card numbers. The system was pathetically easy to crack, but then it had to be readily understood by thousands of long distance operators. Essentially, the calling card number was the billing phone number plus some extra meaningless digits and a letter. The letter corresponded with one of the specific digits in the billing number. So, say the third digit was the key one. The letter at the end had to match the assigned value of that digit. If you had a list of the ten letters for a given year and the location of the key digit, you could make your own fictitious accounts. There were no high speed computers to verify your number and it would work for quite a while until it hit the bot sheets. As mentioned, the codes changed annually, but if you had a friend who was an operator, or perhaps a night watchman in a big office building, you could come up with enough numbers to puzzle it out by early January. Phone security would invariably call the receiver of a bogus card call and ask if they knew who had called them from the originating city. Not a good system if you lived with your parents.

Abbie Hoffman published a lot of this stuff in *Steal This Book*, and after *Esquire* magazine wrote their seminal "Phone Freak" article in the sixties, a lot of it came to an end. Eventually the single hole "Urban Fortress" phones phased out the three-hole phone and we all had to improve our skills to stay ahead of the curve. The rest, of course, is history.

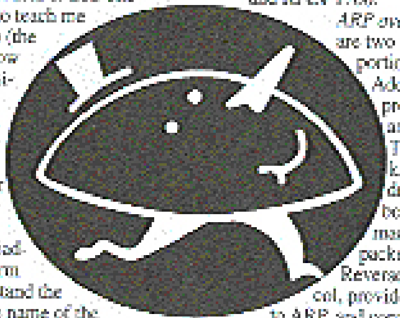
PACKET ANALYSIS AND HEADER SNIFFERS

by Javaman

I decided not too long ago that I wanted to gain a deeper understanding of how internetworking functions on the lower levels, particularly the function and stateful interactions of protocols. After studying several RFCs, writing some code, and asking many questions, I feel much more in touch with the raw data floating across my CAT5 strands than I ever have before. Hopefully this article and the code attached will help you make the same journey.

The reader may ask what he or she may gain from reading this article and examining the attached source. I hoped to target several groups: the novice programmer who wants to learn a form of network coding, the sys/net admin looking to add a few more tools to their kit, and the beginning hacker interested in adding some network level skills to his or her capabilities.

This is a good time to mention that all code here is for educational use only. It was never intended to be the basis of an attack, theoretical or not. The source displayed was written to teach me several things, namely libpcap (the packet capture library used), low level packet analysis, and possibly primitive IDS (Intrusion Detection System) techniques. With that said, let's discuss some basic network concepts, then move to the header sniffer code.



Protocol Introduction

Almost everyone who is reading this article has heard the term TCP/IP, but all may not understand the significance of the pairing. The name of the game when it comes to modern networking is encapsulation. Like a digital matryoshka doll, data transported via TCP is wrapped with a TCP header, which is in turn wrapped by an IP header, which is in turn packaged in an Ethernet header. Not only is this true for TCP, but for any protocol carried by IP, such as ICMP, UDP, and numerous routing protocols. It may be a good idea to eventually commit the size of each header in bytes to memory, which can be determined by writing a simple program. This can be extracted from the code attached.

Each protocol, which has its own associated header, serves a different task. Additionally, each inner protocol adds new functionality. For example, the Ethernet header provides the simplest of addressing (which card on the subnet to pass a packet to), while TCP governs things such as ordered and guaranteed packet delivery, along with multiplexing. This provides future growth in our networks, and is probably the reason why machines that are 20 years old are still capable of communicating on the networks of today, and undreamed of protocols and transmission techniques of today can still work across the majority of the networks.

Because of the length involved and the reality that it would be impossible for me to improve upon the original RFCs, complete specifications on how each protocol works and finite state diagrams for connection-based techniques are not included. This information can be pulled from the RFCs listed throughout the document. If print is preferred, I highly recommend the books written by the late W. Richard Stevens.

General (And Amazingly Brief) Protocol Overview

IP over Ethernet: The lowest layer that we shall be concerned with, the Ethernet frame, defines some basic properties about what our packet is going to look like. The Ethernet header will define the source and destination Ethernet addresses, along with the ethertype, which can be thought of as the data stored inside the headers, be it an IP packet or an ARP request. More information can be found in RFC# 1042 and RFC# 1700.

ARP over Ethernet: ARP and RARP are two components used in transporting IP over Ethernet. ARP, or Address Resolution Protocol, provides a facility to translate an IP to an Ethernet address. This allows a machine to know which gateway to address a packet to if it is outbound of the subnet or which machine on the subnet the packet is destined for. RARP, or Reverse Address Resolution Protocol, provides a complimentary service to ARP, and converts an Ethernet address to an IP. Refer to RFC# 826.

ICMP: ICMP, or Internet Control Message Protocol, is where many functions pertaining to Internet operations, such as dealing with routing difficulties, resides. Facilities such as ping (ICMP_ECHO) operate on the ICMP level. All these protocols have a similar header, with some possessing additional fields, such as Timestamp/Timestamp Reply's three timestamp fields. Consult RFC# 792.

UDP/TCP: Through the use of sockets, UDP and TCP allow for multiplexing of the communication between two machines. Rather than every packet being destined for the IP only, User Datagram Protocol and Transmission Control Protocol allow for an additional address, known as a port. UDP only facilitates this functionality, but TCP goes further. The protocol allows for guaranteed and ordered delivery of data through the use of sequence numbers, a metric unique to the current packet used for identification and ordering, and acknowledgment numbers, which are passed from the receiver to the sender to inform the latter of what the last packet received was. A separate field just containing flags in-

dicating the negotiation and termination of communication is included additionally inside the TCP header. All the fields and flags for TCP are too numerous to mention here. Please read RFCs 768 and 793.

Functionality

By now one may be wondering what the function of the code below is: rather than like most packet sniffers which grab the payload of the communication, this code displays the headers of the protocols only. Why is this useful you may ask? Well, it's simple: examining initial SYN counts, watching badly formed headers drop by, determining sources of attack, etc. I wrote this tool to gain a better understanding of networking in general. Hopefully it will assist you in the same way.

Explanation of Code

The comments in the code make the source rather self explanatory. The program does some variable initialization, command line parameter parsing, and then some libpcap calls to locate the network card. Each packet is then passed to a function called handler(), which then takes the char array (the raw packet), and formats it into something a bit more readable. This may seem oversimplified, but I believe the code contains the best explanation possible. Learning to read source code is an important skill, and is the one by which I learned most of my programming capabilities from.

Keep in mind that libpcap, a cross-platform library, is required for this code. Libpcap can be found at:

ftp://ftp.ee.lbl.gov/libpcap-0.4.tar.Z

To compile the code, enter the following command:

gcc -o headers headers.c -lpcap

This code has to be run as root, since it involves putting an interface into promiscuous mode. As with anything that needs to be run as root, read all the source carefully beforehand. This is just common sense.

If you are really really paranoid, you should be able to chmod your ethernet device to 666, but I would not recommend that on a box with more than one user.

```
/*
 * headers.c, a header analysis tool written by Javaman
 * This software is for educational use only.
 * You have been warned.
 */

/* Numerous includes.  netinet/* is struct definitions and
 * the ntohs/ntohl functions, which are described later.
 */
#include <pcap.h>
#include <stdio.h>
#include <unistd.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <netinet/ether.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>
#include <sys/socket.h>

/* Since the packet handler function is called by pointer,
 * there is no standard way to pass from main() to handler().
 * Because of this, the *dump and *len variables are implemented
 * to store the switch to display various header parameters
 * and the length of headers, respectively.
 */

char ethdump, ipdump, tcpdump, udpdump, icmpdump, arpdump;
char ethlen, iplen, tcplen, udplen, icmplen, arplen;

/* handler() is the function called later by pcap_loop, the
 * actual function that grabs packets off the line.
 * help() is a synopsis of the command line flags to the program,
 * which is displayed for the user by calling the program with no
 * command line options.
 */
void handler (char *, const struct pcap_pkthdr *, const u_char *);
void help (void);

int main(int argc, char **argv)
{

    int bufsize = 65535;        /*Maximum buffer size          */
    int promisc = 1;            /*Promiscuous mode?  Don't mind if I do */
    int timeout = 1000;                   /*Read timeout in milliseconds          */

    char pcap_err[PCAP_ERRBUF_SIZE];
    u_char buffer[255];
```

```
        char i;
        char *dev;
        struct in_addr net, mask;
        pcap_t *pcap_nic;

        /* Initialize all flags at false (0) */
        ethdump = 0;
        ipdump = 0;
        icmpdump = 0;
        tcpdump = 0;
        udpdump = 0;
        arpdump = 0;

        /* Determine the size of each packet. */
        ethlen = sizeof(struct ether_header);
        iplen = sizeof(struct iphdr);
        tcplen = sizeof(struct tcphdr);
        udplen = sizeof(struct udphdr);
        icmplen = sizeof(struct icmphdr);
        arplen = sizeof(struct ether_arp);

        /* If no arguments are supplied, display command line args and quit.*/
        if (argc == 1) {
                help();
                exit(0);
        }

        /* Parse command line arguments with getopt() */
        while ((i = getopt(argc, argv, "ticua")) != EOF) {
                switch (i) {
                        case 'i' :
                                ipdump = 1;
                                break;

                        case 'a':
                                ethdump = 1;
                                break;

                        case 'c':
                                tcpdump = 1;
                                break;

                        case 'u':
                                udpdump = 1;
                                break;

                        case 'c':
                                icmpdump = 1;
                                break;

                        case 'a':
                                arpdump = 1;
                                break;
                }
        }

        /* Find a device capable of sniffing the network.
         * This could be hard coded into the app, or supplied
         * as a command line argument.  Left as an exercise to
         * the reader.
         */

        if (!(dev = pcap_lookupdev(pcap_err))) {
                perror(pcap_err);
                exit(-1);
        }

        /* Attempt to open the card in "pcap" promiscuous mode. */

        if ((pcap_nic = pcap_open_live(dev, buffersize, promisc, timeout, pcap_err)) == NULL) {
                perror(pcap_err);
                exit(-1);
        }

        /* Grab the IP and netmask of the interface into in_addr set and in_addr
         * mask.  This could prove useful later, and is generally valuable
         * information to have.
         */
        if (pcap_lookupnet(dev, &net.s_addr, &mask.s_addr, pcap_err) == -1) {
```



```
                perror(pcap_err);
                exit(-1);
        }

        /* Now we are ready to grab raw packets.
         * pcap_loop runs until a SIGINT is raised (ctrl-C) by
         * grabbing data from interface defined in pcap_nic and passes
         * the data to the function called in the third argument.
         * The parameters passed to this function, handler(), are discussed
         * below.
         */
        while (pcap_loop(pcap_nic, -1, (pcap_handler)handler, buffer))
                ;
}

void handler (char *arr, const struct pcap_pkthdr *header, const u_char *pkt) {
        /* Pointers to structures for the headers of different packet types.
         * The pointer to the raw packet, expressed as const u_char *pkt,
         * is going to be cast to the individual structs (with an offset
         * for each packet) to facilitate easier manipulation later on.
         */
        struct ether_header *ethheader;
        struct iphdr *ipheader;
        struct udphdr *udpheader;
        struct tcphdr *tcpheader;
        struct icmphdr *icmpheader;
        struct ether_arp *arpheader;
        struct in_addr source, dest;
        int y;

        /* This is the first test, and it assures that all packets coming
         * down the line are proper Ethernet packets.  This is a test
         * assumption.
         */
        ethheader = (struct ether_header *) pkt;

        /* If dumping of Ethernet packets is specified, print the source
         * and destination Ethernet (MAC) address, along with the ethertype.
         * The ethertype can be thought of the protocol encapsulated
         * by the Ethernet header.
         */
        if (ethdump) {
                printf("\nEthernet\t");
                for (y = 0; y < 6; y++) {
                        printf("%02x", ethheader->ether_dhost[y]);
                        if (y!=5) {
                                printf(":");
                        } else {
                                printf("\t");
                        }
                }

                for (y = 0; y < 6; y++) {
                        printf("%02x", ethheader->ether_shost[y]);
                        if (y!=5) {
                                printf(":");
                        } else {
                                printf("\n");
                        }
                }

                /* The call to ntohs() is to convert the byte order from network
                 * (big endian) to host (which in most people's cases is going
                 * to be little endian).  This will let the data dumps
                 * make sense.
                 */
                printf("Proto: %04x\n", ntohs(ethheader->ether_type));
        }

        /* If the ether type is 0x0800 or it is 0x0835, then the packet is
         * either an arp or a RARP packet.  This is how machines translate
         * an IP address into a MAC address (arp) or vice-versa (RARP).  The
         * latter is used by x-terminals to discover their IP address, for
         * example.  The reason why the constants appear reversed is to show
         * the effect of network byte order without calling ntohs().
         */
        if (arpdump && ((ethheader->ether_type == 0x0608) || (ethheader->ether_type ==
0x3580))) {
                /* Another cast to a packet type. */
                arphdr = (struct ether_arp *) (pkt+ethlen);
```

```
		/* The memcpy() is just to place the ether addresses in a slightly
		 * easier to remember place.
		 */
		memcpy(&source, &arppkt->arp_spa, 4);
		memcpy(&dest, &arppkt->arp_tpa, 4);
		printf("\nARP:\n");
		printf("%04x %04x\n", ntohs(arppkt->ea_hdr.ar_hrd), ntohs(arppkt->
ea_hdr.ar_pro));
		printf("%02x %02x %04x\n", arppkt->ea_hdr.ar_hln, arppkt->ea_hdr.ar_pln,
ntohs(arppkt->ea_hdr.ar_op));
		for (y = 0; y < 6; y++) {
			printf("%02x", arppkt->arp_sha[y]);
			if (y!=5) {
				printf(":");
			} else {
				printf("\n");
			}
		}

		for (y = 0; y < 4; y++) {
			printf("%02x", arppkt->arp_spa[y]);
			if (y!=3) {
				printf(".");
			} else {
				printf("\t(%s)\n", inet_ntoa(source));
			}
		}

		for (y = 0; y < 6; y++) {
			printf("%02x", arppkt->arp_tha[y]);
			if (y!=5) {
				printf(":");
			} else {
				printf("\n");
			}
		}

		for (y = 0; y < 4; y++) {
			printf("%02x", arppkt->arp_tpa[y]);
			if (y!=3) {
				printf(".");
			} else {
				printf("\t(%s)\n", inet_ntoa(dest));
			}
		}
	}

	/* If the ethertype is 0x0800, the encapsulated data is IP.
	 * Good: the good stuff is below.
	 */
	if (ethheader->ether_type == 0x0008) {
		ipheader = (struct iphdr *) (pkt+ethlen);

		/* If the user selected to see the IP header and it is ipv4, then
		 * dump the IP header.  IPv6 would be easy to add, and is left
		 * as an exercise to the reader.
		 */
		if (ipdump && (ipheader->version == 0x04)) {
			memcpy(&source, &ipheader->saddr, 4);
			memcpy(&dest, &ipheader->daddr, 4);
			printf("\nIP:\n");
			printf("%1x %1x %02x %04x\n", ipheader->version, ipheader->ihl,
ipheader->tos, ntohs(ipheader->tot_len));
			printf("%04x    %04x\n", ntohs(ipheader->id), ntohs(ipheader-
>frag_off));
			printf("%02x %02x  %04x\n", ipheader->ttl, ipheader->protocol,
ntohs(ipheader->check));
			printf("%08x    (%s)\n", ntohl(ipheader->saddr), inet_ntoa(source));
			printf("%08x    (%s)\n", ntohl(ipheader->daddr), inet_ntoa(dest));
		}

		/* Same as above, but for UDP headers.  Inside the IP header
		 * there is a protocol field, which specifies if the payload
		 * is UDP, TCP, ICMP, EGP, or a host of protocols.  You can
		 * find the full list in RFC #1700, Assigned Numbers
		 */
		if (udpdump && (ipheader->protocol == 0x11)) {
			udpheader = (struct udphdr *) (pkt+ethlen+iplen);
			printf("\nUDP:\n");
```



```
			printf("%04x %04x\n", ntohs(udpheader->source), ntohs(udpheader-
>dest));
			printf("%04x %04x\n", ntohs(udpheader->len), ntohs(udpheader->check));
		}

		/* Again, same as udp, but for tcp */
		if (tcpdump && (ipheader->protocol == 0x06)) {
			tcpheader = (struct tcphdr *) (pkt+ethlen+iplen);
			printf("\nTCP:\n");
			printf("%04x %04x\n", ntohs(tcpheader->source), ntohs(tcpheader
->dest));
			printf("%08x\n", ntohl(tcpheader->seq));
			printf("%08x\n", ntohl(tcpheader->ack_seq));
			printf("%1x %02x %1x:%1x:%1x:%1x:%1x:%1x %04x\n", tcpheader->doff,
tcpheader->res1 + tcpheader->res2, tcpheader->urg, tcpheader->ack, tcpheader->psh,
tcpheader->rst, tcpheader->syn, tcpheader->fin, ntohs(tcpheader->window));
			printf("%04x %04x\n", ntohs(tcpheader->check), ntohs(tcpheader-
>urg_ptr));
		}

		/* This subsection is for ICMP.  The separate individual if's encompass
		 * the two general forms of ICMP headers.  A full list of ICMP headers
		 * can be found in RFC 792.
		 */
		if (icmpdump && (ipheader->protocol == 0x01)) {
			icmpheader = (struct icmphdr *) (pkt+ethlen+iplen);
			printf("\nICMP:\n");
				printf("%02x %02x %04x\n", icmpheader->type, icmpheader
->code, ntohs(icmpheader->checksum));
			if ((icmpheader->type == 0x08) || (icmpheader->type == 0x00) ||
(icmpheader->type == 0x0d) || (icmpheader->type == 0x0e) || (icmpheader->type == 0x0f) ||
(icmpheader->type == 0x10)) {
				printf("%04x %04x\n", ntohs(icmpheader->un.echo.id),
ntohs(icmpheader->un.echo.sequence));
			} else if (icmpheader->type == 0x05) {
				printf("%08x  GW: %s\n", ntohl(icmpheader->un.gateway),
inet_ntoa(dest));
			}
		}
	}
	return;
}

/* The help function describes the various command line options
 * supported at this time.
 */
void help(void)
{
	printf("Headers by Javaman v1\n");
	printf("For information purposes only.\n");
	printf("Options:\n");
	printf("\t-e\tDump Ethernet header\n");
	printf("\t-a\tDump ARP/RARP info\n");
	printf("\t-i\tDump IP header\n");
	printf("\t-c\tDump ICMP header\n");
	printf("\t-t\tDump TCP header\n");
	printf("\t-u\tDump UDP header\n");
}
```

Conclusion

Hopefully this tool has helped introduce the reader into some basic concepts of low level IP operation. This snippet can be added to to provide some basic IDS functionality, and possibly a tool for other, as of yet unimagined projects projects.

Pertinent Links

RFC Database: www.faqs.org/rfcs

This has been where I have been reading my RFC's from. Libpcap: ftp.ee.lbl.gov/libpcap-0.4.tar.Z

The code was written using libpcap v0.4. Hopefully by the time this article is published, the code will not be updated, just for simplicity purposes only. Philtered.net: www.philtered.net

The code contained in this article can be downloaded from this site, with no comments, of course. If you want commented code, buy this magazine. Additionally, my e-mail address along with other projects from our group can be found.

RFC List

RFC 768: User Datagram Protocol, RFC 791: Internet Protocol, RFC 792: Internet Control Message Protocol, RFC 793: Transmission Control Protocol, RFC 826: Ethernet Address Resolution Protocol, RFC 1042: Transmission of IP Datagrams over IEEE 802 Networks, RFC 1700: Assigned Numbers

DANGEROUS THOUGHT SECTION

Clarification

Dear 2600:

I really respect what you guys do and the rights of hackers that you stand up for. I do believe that you have a bad view on what a hacker is. I hate to break it to you, but a cracker is a hacker. These recent attacks were hackers. I bet you're shaking your head right now but it is true. Every group of people has its bad people. There are bad priests, doctors, and lawyers so why can't you guys just agree with that instead of trying to make two separate groups, hackers and crackers? We all do the same thing: mess with computers and the like. If you call Jack Kevorkian a doctor, the other doctors don't get mad and say "He's not a doctor, he is a murderer." Some may say that but the majority still believes that he is a doctor. I do understand that you would like people to stop viewing all hackers as bad, but in the age of morons that is impossible.

Kevin V
Trenton, OH

We don't know where you got the idea that we want to perpetuate this "cracker" nonsense. We believe the word does a great disservice to hackers everywhere as it criminalizes without explaining the crime and the end result is that the uninformed get a mostly negative view of the hacker culture. We also don't know how you're so certain that these recent attacks were the work of hackers. It's been widely reported that anyone with the right script could have done this. Is anyone who can type a command to be considered a hacker? We recognize the possibility that it could have been a hacker but it's really irrelevant as it's as much an act of hacking as cow tipping.

Dear 2600:

This message is in reply to a letter posted by Desaparecido in 16:4. In his letter, Desaparecido claimed that it is an elitist group of "hackers," or those who "have the knowledge" who actually have the "power." It is my belief that by stating this, he is creating a sense of an aristocracy (one that obviously does not exist) between the elite (hackers) and the rest (society). This is not true and such images should be avoided! If we are seen as elite/elitist, or aristocratic, then we are just as damned as the "powers that be" (government). We must strive to show society that hackers are no different from the common man, that they do not wield any hidden weapons, or for that matter any *hidden* knowledge. Assuming that the goal of hackers is to create a free and informational future for mankind, an elitist view would create an exact opposite result. So, in conclusion: Desaparecido had the right idea, but used the wrong word! "We" should not be separated from "them."

Treker

Dear 2600:

In regards to what Black Knight had written in 16:4. He is either a Seal wannabe or a Seal. Only Seals say dumb things like that. I don't see a reason for honoring the U.S. Navy Seals. If we are going to honor someone in the armed forces it should be all branches of the military because no matter how little or how much work each and every one of them do, without one another the job wouldn't get done. They all work as a team.

Einstein

We've started a tidal wave here, haven't we?

Dear 2600:

Just kind of wondering how come when I typed www.fucknbc.com it didn't hit 2600's web site but instead hit NBC's. I know that you guys were getting sued for owning the domain name but I didn't think that you would give it up that easy. I suppose one lawsuit a year is enough, huh? Understandable, I guess.

Mark

No matter what we did on this, people thought we were giving in. Initially we had the site pointed to NBC. Then they threatened us with legal action. We pointed it to our site so that people would see the story, not because they told us to. After people started to think that we were pressured into that, we pointed it right back to NBC. Then people somehow thought we were pressured again. So, to make matters simple, we've pointed fuckabc.com to CBS and fuckcbs.com to NBC. Hopefully, this will make everyone happy. We should point out that CBS has taken the existence of our site a lot better than NBC. Of course, their parent company (Viacom) is already suing us for DeCSS. We hope to have some more permanent sites in place that will do more than point in the near future.

Dear 2600:

There has been a number floating around the Houston area in the past couple of months. It is supposedly a number to call to detect a tap on your line. As the story goes, if your line rings busy, it is tapped. Otherwise it gives you a weird musical sound. The number is 817-284-7847 (or 817-BUG RUGS). I don't really believe all of the hype but I was wondering if you would give it a ring and give me your opinion.

Transmissions from the South

This comes up every couple of years. There are no such numbers. The easiest way to prove this is to tap yourself and see if you notice a change. The number, incidentally, goes to a sweep tone which, if someone were tapping you, would annoy them no end if you called it for long periods of time.

Getting Around Stupidity

Dear 2600:

A while back I was using a school computer that had a filtering system enabled. It was intended to filter out porn, bomb-building techniques, and other miscreant information. Intriguingly, it also blocked 2600, which seems to have become the norm for filter programs these days. Not easily dissuaded, I tried some different variations, and found that 2600.net, .com, and .org were all blocked. But *aha!* Country codes! God love the Canadians because 2600.ca was wide open. It's got to be the easiest way to get around those pesky filters.

Dr Jest

That's one of the reasons we encourage people from other countries to get the 2600 domain and point it our way. In exchange, you'll get a subscription for as long as it stays up. And don't forget to try www.2600.middle-island.ny.us as well. Almost no one thinks to block that one.

Dear 2600:

I was using the computers at school which run CyberPatrol. Screw hacking it when all ya have to do is use an anonymous proxy server. I went to www.aixs.net and surfed all I wanted. Let's see CyberPetrol try to block the proxy servers now. Ha ha!

Karr0t T0p

You think they won't try?

Dear 2600:

I just found an interesting bug in the blocking software that my library uses to unblock sites that don't deserve to be blocked (as well as ones that should). The trick is this: after you type out the URL, you add ":80" after the .com to specify the port address. That seems to be the default port address, and allows you to get in.

phil

Dear 2600:

I work for a company that has your 2600.com domain banned in its proxy. In fact, someone let you know of this in the letters section of a previous issue. We get a big red graphical stop sign and a note saying this site is known to pose information security risks and contains possible computer viruses.

Aside from expressing your rights to comment on the quality of the company, your registering of the domains like verizonREALLYsucks.com and the more creative VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com also provides a workaround for those of us who wish to stay updated by reading the newsbreakers of your web site while at work (on breaks of course).

sonnik

A side benefit we hadn't even thought of.

Dear 2600:

Well as many of you know Metallica has their panties in a wad about MP3s and the service of Napster. Recently about 300,000 or so people were banned from Napster. This happened to a friend of mine. He would try to register a new name and it wouldn't let him. Well, his cousin was poking around the Windows registry and found something that Napster put there. He simply removed it and got a new Napster name. If you know your way around the registry, just poke around - it's in there somewhere.

GhettoBlaster
(formerly Jason Louisiana)

Discoveries

Dear 2600:

In a letter a while back on Citibank ATMs, you guys had someone ask what the "Undocumented Feature" was. After taking about two hours to figure it out I realized that if you use the seeing impaired function you are not charged the $1.50 surcharge for using their machine as opposed to using the standard function. Just thought you would like to know. Also, I asked the bank manager and was thrown out of the office. Oh well. Thanks.

Squee

Dear 2600:

I have been meaning to pass this on for some time now. The default password for AT&T cell customer voice mail boxes is 1111. We found this out when Hurricane Floyd sunk what was at the time our local exchange.

Allin

Dear 2600:

Recently I visited www.ask.com for the hell of it and when I got there my mind was at a loss for questions to ask him. Eventually my mind began to wander so I typed "Is Jeeves gay?" and almost immediately (due to my 56k) the results popped up. Under the section "I have answers for:" the first one was "Is Jeeves gay?" so it struck my curiosity and I clicked on it. The resulting page displayed:

429 File None of Your Business

This file is none of your business. You have a lot of nerve even clicking on this link.

This made me happy because even though it's a crappy search engine, it still has a sense of humor and that's what's missing in the technology world of today. After that uplifting discovery I decided to make Jeeves one of my most frequently used engines. Thanks Jeeves.

Elektr0chr0nik

We wonder what the results would have been had Jeeves really come out of the closet. Would fundamentalists start boycotting it?

Dear 2600:

A few months ago I got arrested for some traffic warrants that were building up for a couple of years and I noticed the laptops that authorities are utilizing in the squad cars. I had read briefly about them but never saw one. I only noticed that it was a Panasonic laptop and had what looked like a real "stripped down" look to it. OS speaking. As if it were almost a "nix system. But by talking to the officer, I eliminated that idea as he was too fucking stupid to use an Atari. Unfortunately, I was picked up at 7:00 in the morning and could not see well without my contacts. But he did mention that it used radio frequency and not cellular and the network that they used for this communication was "tac Fix." This is not how it is spelled but I had

never heard of that network/company so I spelled it the way it sounded.

My second encounter happened after coming home from a nightclub in Dallas. My roommate's car was broken into and the CD deck was stolen. Of course, we called the police to get a report so his insurance would pay for it. When the officer arrived, I noticed the laptop again. I have to admit that the officer was extremely friendly but not too informative. I asked a couple of questions about it and he finally offered for me to "jump in and check it out!" Uhmmm... OK. So here I am at three in the morning, *drunk off my ass*, sitting in the driver's side looking at his laptop without supervision.

This laptop was Motorola and highly customized. Touch screen with a Windows NT 4.0 platform. He said that they use the "tee lits" network for the communication but was unsure about the means of transfer. And I forgot to trace the cable to find out myself. D'oh! But I'm positive that tracking software currently used is Tiburon (as in shark) by Maco (possibly misspelled) or the other way around. Again, I apologize for the lack of consistency as I was drunk. No "spooning" as it just flashed and died. He mentioned that they do send e-mail back and forth so I assume it's Internet protocol related.

bill

We're glad to see people continue the quest for knowledge even while under stressful conditions. It's an extremely valuable skill to have.

Car Talk

Dear *2600*:

In 16:4 you published a piece titled "I Own Your Car" by Slatan. In the story the author claims to have worked for "one of the most prestigious car companies." It's fairly obvious to me that the article is about the Cadillac Evoq, a vehicle which was a concept car that GM has put on a track for production. The Evoq has been portrayed in the press as being "Cadillac's Corvette" and will also reportedly share some mechanicals with the Corvette. The "night vision" the author refers to is available as an option on current Sevilles. The onboard navigation system he references sounds a lot like GM's OnStar system which is available on many of GM's luxury vehicles. I personally know people who build show cars and prototypes for General Motors, and the author's assertion that he got access to six of them, let alone was able to drive one off of the premises, is ludicrous. Even assuming that this story is true, anyone who would jump into a prototype vehicle that they have no personal knowledge of, drive it at speeds of "over 150" and come off of an exit ramp on I-75 (a road I travel regularly, sometimes in the early morning hours described in the article) "at 75 mph" is a complete asshole. Sometimes certain prototype cars are meant for photo or display use only, and if the author's story was true then he endangered others on the road, especially when this dumbass "flipped off the headlights." However, I think that this story was complete bullshit, as the Evoq has been in the press for a long time. To read more about the Evoq at *Car & Driver* go to www.caranddriver.com/FrameSet/0,1550,_sl_NewArticle_sl_0_cm_1655_cm_2321_1_16_cm_0,00.html.

Devil Moon

Dear *2600*:

In response to the article "Hacking Explorer (the car)" by Bob in 16:4, the keyless entry system techniques he outlined should work on any Ford keyless entry system. I can personally verify that along with the Explorer, these sequences also work on the Windstar minivan models. Additionally, after entering the five digit code and unlocking the driver's door, you can press the {3-6} key to unlock the trunk or equivalent. Besides Ford models, I can verify from experience most of these keyless entry system sequences also work on the Mercury Grand Marquis.

The Artful Dodger

Annoyances

Dear *2600*:

Russ was complaining in 16:4 about how inconsiderate folks can be with their cell phones. There's a company in Israel that produces boxes which jam cell phone signals and, while they don't list prices on their web site, I'm sure it's worth it if you've had it with the mobiles. The company is Nedline Technologies, and they can be found at www.e-guard.com.

thegeek
Glasgow, Scotland

That's one technique. Here's another.

Dear *2600*:

Don't know if anyone has tried this. I was on the bus today and overheard some man talking on his phone (loudly enough for everyone to hear). While he was talking I wrote down some of what he said. I got name, address, phone number, place of work, and other good stuff. When he was done I started up a conversation with him. Addressed him by name and asked how his new apartment was. He was dumbfounded. I shared with him what he just told the rest of the bus and he didn't even realize it. Neat.

Funk Strings

Dear *2600*:

I just want to say this magazine is by far the most intellectually stimulating thing I can find in bookstores today. Anyway, I was just reading the issue I got today (love the Looney Toons cover) and it wasn't on the shelf. I looked in every part of the store, even in the computer book section. I asked the clerk at the front if they carried the magazine. He said, "Yeah, not a lot of people really buy it though." After about five minutes of waiting, it came up to the front bundled in the rope it was shipped in. He said, "You wanna buy these, all we're going to do is throw them out." I said, "Really." He replied, "We'll return them, of course." I said, "Let me see 20 of those." He handed them to me and I went straight to the magazine shelf and put them there. God, people like that really piss me off.

2MnYiDiZ

We appreciate your help. It's amazing the efforts people go to to make sure we get on the shelves. It's also pretty sad how hard others try to keep us off them. When things like this happen, let us know the exact locations so we can follow up and make sure they don't continue to do these evil things.

Dear *2600*:

Melissa was the warning to which Micr*s*ft obviously did not listen. Now there is Smash (the ILOVEYOU virus), which eventually wipes out your hard drive. My corporate e-mail has been shut down as a containment measure. As I understand it, this virus infected *thousands* of exchange networks in the U.S. in just one day! What is it going to take to get big corporations to realize that Micr*s*ft can hurt them? The sad reality is, they won't listen until their networks are infected by a virus that simply wipes out everything, and productivity takes a nose dive. I just hope I'm not around when they start firing people because they don't know what to do.

ryan

Someone ought to write one of those things that simply replaces Microsoft Outlook with something secure. That would be a public service and might put an end to the stupidity we've all had to endure in the media on this topic.

Retail Tips

Dear *2600*:

In response to Creature's letter concerning the touch screen POS systems used in Ruby Tuesday: most Ruby's that I know of use a Micros 2800 system. These employ a proprietary operating system stored on a flashable rom chip. All the workstations work as individuals that broadcast changes as they are made to the rest of the units on the system. Most Ruby's will have a Win 9x box in the office that attaches to the Micros machines for reporting and credit card processing.

The interesting thing about the 2400 and 2800 series Micros systems is that the manager mode is entered with a key or a swipe card. If you have access to a terminal, remove the back cover, then remove the two screws holding the top cover in place. Look for the connector that the key-switch connects to. Use a paper clip (or any other conductive material), replace the cover, and you too can be a manager. From the main screen, holding shift and enter will take you to manager mode. From here you can have all sorts of fun: free food, altering of prices, deleting employees, etc.

SnoFlak

All of which practically guarantee you'll be caught really quick.

Dear *2600*:

Cheers to all those people out there who have enough courage to come forward and expose the secrets of so many chains. We should all applaud the risk they are taking and their willingness to do it nonetheless. Hopefully, all those stores that have been overcharging us, the consumers, for years will finally see that if they don't change their ways the consumers will strike back. I hope you, the good people at *2600*, will continue to print these articles as well as ignore the idiotic requests of these stores.

gas fumes

More like demands, you mean. But we don't print information for the purpose of revenge. We print information, period. We like to learn about how things work. We don't advocate using what we print in a destructive way, even when it may appear to be justified.

Dear *2600*:

This is in response to Phelix who asked about Pizza Hut's SCO Unix-based POS system in 17:1. I've worked with a few SCO-based POS systems, but all of them have a common thread (at least from what I have seen). Most SCO-based POS systems come from a company called Infinite Solutions in Atlanta, GA. (Infinite Solutions also markets themselves under three different company names and was recently bought out by a company called Savior Technology Group). They're used by a lot of bridal/tuxedo shops, hotel chains, and pizza places because of the database backing that these systems can do. Pizza Hut, Papa John's, WH Smith Hotels, and Domino's Pizza are some places that use this type of system.

There are two ways that these systems are set up in stores. One of which is where they have one server and cash registers. The cash registers are "polled" to the SCO Unix server via a modem at night. In some stores, a bunch of registers are connected to one modem via an IRC Cable (yes, really, that is the name of it). Then, after all the registers are done polling, the server dials up the home office and transmits data (usually at 9600bps eeeek!). All of this is done via cron jobs.

The second way these systems are set up (mostly for pizza chains), is where they have one SCO box in the store and dumb terminals around the store. The SCO Box usually sits in the manager's office with a 33.6 fax/modem attached to it. At the end of the day, the on-duty manager enters their cashier PIN in and it processes the daily sales, then dials the home office and transfers sales.

The only difference is that at least one of the companies I have worked for has switched from modems to a networked ISDN system. (Some stores have *very* large sales databases that need to be transferred at night and it just take too long over a modem.) This will only make the work for you harder.

The modems in these SCO boxes are also used for administrative purposes from the home office, or Infinite Solutions. Usually when you purchase one of these POS systems you are required to purchase (expensive) yearly support for these. This is because most of the time, the store does not own the hardware or OS that the POS system runs on and just owns the sales data. (Dumb idea, huh.) This is so they can, as Infinite Solutions puts it, offer premium customer service and support. *(Big joke.)* Usually when you dial up, you get an SCO

SysV login prompt and that's it. The modem connection is straight tty device (so easy to hack). And the sales data that is sent via the modem is done so via UUCP (I find it hard to believe it's still done this way). The only problem with some systems is that in some store setups, the modem is *not* set up for AA (auto-answer), so you may not be able to dial directly into the machine. (Administrative things are done by having the manager of the store make the modem dial out to the home office, instead of the home office dialing in.) As far as logins, usually the home office and Infinite Solutions have administrative logins that give you direct access to the login prompt. *And* when you dial up into the SCO box, it *does* allow for root to be directly logged into! (dumb dumb) The logins to the system that are administrative can vary from company to company. And it's the same for the root password. Usually, when Infinite Solutions has to do support on the box, they call someone at the home office to get the root password and login. Infinite Solutions usually has a non-root login to every box though, just so they can poke around. (It's usually "infinite".) The other way around this, if you don't want to try the modem route, is to get a cashier passcode for the store manager or a district manager. These types of passcodes have extra features than the normal cashier logins. This is so managers can run reports and do weekly system maintenance and backups. And on some versions of the POS system, you are allowed to exit to a SCO prompt!

OK, so you've gotten into the system. Now what? And to me it would be more like "Why?" The thing about it is that most of the SCO boxes have most compilers and system tools taken off. There is usually just enough stuff on there to run the POS system, the database that backs it, and some minor administrative tools. Hell, even "useradd" doesn't exist on most of these systems. What is on the system depends on what package the company decided to purchase from Infinite Solutions.

I hope this helps you in your journey to hack a Pizza Hut POS system.

Cybah

Additional Info

Dear *2600*:

I just wanted to say that in addition to the programs listed in "Killing a File" (16:3), another one that can be used to clean-wipe a file is none other than the popular encryption program PGP. To make a more secure delete, you can encrypt a file and then use PGP's Wipe feature to clean-erase it. It renames the file to all A's, rewrites over the file's contents, and then overwrites the file completely.

Immolation

Dear *2600*:

MMX might want to mention that mini DMS's or mini CO's or whatever you call them in the U.S. interfere with the test of a line to the point where inaccurate readings will leave the inexperienced lost.

mbve

Dear *2600*:

After reading the article by Prototype Zero on the Sprint ION network I thought I would send some corrections. I have been working on the ION project for nearly a year and have to tell you first of all ION is scheduled for general availability in April in Kansas City, Denver, and Seattle. Next, I have to tell you that Cisco is not even a major vendor in the ION network. The DSL DSLAM at each of the CO cages is using a Lucent Stinger and the CPE side is a Sprint internally developed device. Next, the voice lines are not unlimited. The plan was to make up to four phone lines available per customer. As of last month they were only able to get two to work. Some of the problems with the implementation is that it is Voice over IP over AAL5. The quality of the sound is similar to talking over a couple of soup cans on a string. These problems will be corrected when they start using AAL2. Oh yeah, and since the beta test they discovered the Network Neighborhood problem. You know, the one where you can browse your neighbor's computer. Other parts of the country that are not going to have ION but will have DSL access include but are not limited to Florida and North Carolina.

Qwertydvorak

Dear *2600*:

I am responding to Handle6015's letter in 17:1. What you stumbled on is Timbuktu, a remote access program. It allows TCP/IP, AppleTalk, or Dialup access to another computer. Look mode lets you see the other computer's screen, control lets you do whatever you could if you were at the computer. I know it's for Mac. No idea if they make it for another platform.

DAR

Dealing With The MPAA

Dear *2600*:

What effect do you think we, the customers, could have on the MPAA if for one month we boycotted purchasing movies and music? As hard as it might be to do, it may be necessary to show them how we feel. You have to hit them where it hurts.

Scott

While it would be great to be able to show this kind of force, we have to face the fact that the vast majority of people aren't aware of the facts in this case and have no idea how they're being manipulated. So, in addition to a boycott not being feasible, we wouldn't actually be proving anything since so many people still wouldn't know what it's about. Our strength and energy needs to be directed towards educating people in one place at a time. It's a daunting task but it does work. We've already made a great deal of progress since the beginning of the year. A boycott will be far more effective after we've reached even more people.

Dear *2600*:

It was only a matter of time. After all the bruhaha over DeCSS someone has finally created a legal DVD player for the Linux platform. LinDVD has been created and will be marketed by Intervideo for $29.95 and will be available this spring. Hope this helps you out some.

Sys Edit

That's all fine and good but it doesn't solve the problem. The very concept of a "legal" player on certain platforms is absurd. Consumers own the hardware, they've bought the software... to require any more from them is, quite simply, wrong. If you can get your toaster to play DVDs, you have every right to, assuming you bought the toaster and the DVD.

Dear *2600*:

This is for Mr. Jack Valenti of the MPAA concerning the DVD FAQ on www.mpaa.org:

"What is the DVD Content Scramble System (CSS) and how does it work?

"CSS is the copy protection system adopted by the motion picture industry and consumer electronics manufacturers to provide security to copyrighted content of DVDs and to prevent unauthorized copying of that content. CSS is akin to the lock on your house."

This is a lie. CSS does not prevent the copying of DVDs in any way. Traditional encryption methods are not capable of protecting data if the viewing platform is going to decrypt it without requiring a key. What you claim is possible but it is far more advanced than simple CSS.

Through lies and propaganda you have convinced the public, and even the courts that through cracking, CSS hackers can now duplicate and distribute pirated DVDs. (Ally enough, you are not, to my knowledge, suing manufacturers of DVD burners that employ bit-by-bit copying. These devices *do* facilitate the copying of DVDs. The reason you are not attacking those manufacturers is simple. You attack only the weak.

You are mistaken if you believe you can stop the "hacker" community. They create, sustain, and promote modern technology. Technology is the most powerful tool in the world today, and you are fighting people who understand it better than anyone.

mr. blonde

Well said. Being thought of as weak does have its advantages.

Dear *2600*:

This can't be happening. Eight corporations have united to shut down *2600* once and for all. We have no rights anymore, so you will probably lose as the judges are on the side of the big guys, but be assured that hackers everywhere will keep up the fight. What's next? Will there be a list of government (i.e., corporate) approved web sites that we have to look at? If you look at a nonapproved web site, will the FBI drag you away and have you executed? Will we only be able to perform government approved actions with computers? It's getting apparent that the big guys want total power, nothing less. They want to control your lives like Pol Pot controlled the lives of Cambodians. The only consolation is that America will probably have a civil war, break up, and become about as stable as Russia. Starving to death amid ruins is not an enticing idea, but we can laugh at the corporations who will have to lie in the bed they made. How can I help before I too "disappear" one day and am never seen again? Oh yeah, I've decided it's too dangerous to use my old handle and real e-mail address, so I set up this one.

Mr. Roboto

The best way to help is to get the word out to the many millions who only know what they've seen in the mass media. That means virtually anyone you talk to will learn something from you.

Dear *2600*:

I am a recently hooked reader of your magazine, and have found it both informative and entertaining. I was appalled to find out about the MPAA case against you guys. I have tried my best to spread the word about both the case and your magazine to everyone I can talk to. Recently at our local movie theater I was passing out some flyers. The manager came out and asked me what I was doing. So I explained about the case and what was going on. To my surprise he took my side and we now have flyers posted all throughout the movie theater, including one in the ticket booth. I gave him some flyers and he said he would pass them out if anyone asked about the posted flyers. I thought that was pretty cool. Just thought I would share.

Jedi's Chaos

Sometimes it's all in how you present your case. One thing is for sure - people with clues are out there and they deserve to be acknowledged when they stand up.

Dear *2600*:

I have been reading *2600* since I was a freshman in high school when one of my older brother's friends handed me a copy of your magazine and said, "Educate yourself." I am now a freshman in college and have been enjoying your magazine for the past four years. I just wanted to let you guys know that you have done a great job keeping me informed and that I have repeatedly had to come to the aid of the hacker name when people use it in a derogatory manner. Also, thanks to your online ordering, I don't have to scrounge through the magazines at the bookstore anymore. I've finally gotten off my ass and ordered a two year subscription. Keep up the good work, and fuck the MPAA! Oops, I hope they didn't hear me, I wouldn't want to be sued.

Daewoo

No, we doubt you'll be sued but we can almost guarantee they'll bring up comments like that at the trial in an effort to show how we constantly deride them and wish evil upon them. The fact is that we don't - it's entirely their arrogant attitude towards the very people who keep them in business (that would be the consumer) that provokes such hostile remarks. We believe a mere glance at the court transcripts (available online at www.2600.com) will invoke more bad feelings towards the MPAA (and the major corporations they represent) than anything we could say. Also, in case you missed the announcement, our trial has been scheduled for July 17 in New York - the day after H2K! We hope to see many people stay in

New York for the fun.

Dear *2600*:

I just started hosting your DeCSS files and read some of the letters the MPAA sent to others telling them to remove the files from their servers and release the identity of the person responsible for hosting them. I was wondering, if I were to receive a letter like this, would I be legally obligated to give them my personal info?

g00fy

You're not obligated to do anything until a court of law tells you to. These letters are meant to get you to buckle or, ideally, frighten someone above you so that they do the MPAA's dirty deeds for them.

Dear *2600*:

What exactly is the argument? When you buy a DVD (or anything else for that matter) it's yours. Therefore you should be able to do whatever you please with it. You should be able to watch it on a computer or see a European DVD on an American player. Why is it that you are being sued for helping people do this?

steve n az (heretic/pogo)

It's a very good question. The short answer is that they're trying to change the rules. When you buy something, they want you to be merely buying a license to use it as they decree you should. That means you would have to accept all kinds of conditions, like not having the ability to skip over commercials. (If you figured out a way to do this, you would be in violation of the contract and subject to what we're facing.) What's interesting is that the MPAA and the film studios had to deceive the courts and the public by claiming this was about piracy when that was not the issue at all. Either they don't understand their own case or they realized just how far they would get by telling the truth.

The Mitnick Case

Dear *2600*:

My husband and I enjoy your magazine immensely (in fact, you're partially responsible for our being married in the first place... but that's another story). We've followed Kevin's case through you and have attempted to educate all who would listen, and we're relieved that he's finally free.

One question has continued to bother me in recent months - where the hell was the ACLU during all of this? I've searched both the Southern California and the National web sites, and there is no mention whatsoever of Kevin's case. When has there ever been a more cut-and-dry violation of the 5th and 6th Amendments? Was this not worthy of their attention? They must have been contacted and they must have responded in some way.

On a lighter note, my six-year-old daughter (already quite computer literate) has a CD-rom game called "Gus Goes to Cybertown." While it's a fairly cheesy title, I was delighted to discover that at one point in the game, a little "CyberBuddy" pops up from behind something-or-other and declares, "Hackers are people who *love* to experiment with computers!"

Destigmatization has finally begun, and at the kindergarten level, no less!

Sienne (805)

Yet another way we've managed to subvert the youth. As for the ACLU, yes, they were contacted regarding Kevin Mitnick, as was the EFF, Amnesty International, and every other organization we could think of. The reasons for not getting involved differed, from not wanting to condone Mitnick's actions (however minor - he was still considered a "criminal" and that's enough for most people) to not having the ability to figure out all of the technical nuances of his case. The latter actually worries us more since it's now possible to lock someone away for five years simply because people don't understand the technology. Don't think we've seen the last of that tactic.

Dear *2600*:

One day I was walking home from a friend's house and I saw a flyer taped to a power line. Lo and behold it was a "Free Kevin" flyer. It was half ripped off so I only saw a picture. I was amazed. The odd part is that it was like a block away from my house. No main roads anywhere. You see, I live in Jeffersonville, Indiana. The city can be summed up in one sentence: "This place is stuck in the 50's." I am so shocked to see that the Kevin story got this far. I mean we still have Apple IIe's in the computer lab at school for god sakes. You got the word out - good job.

Technomatrix

We helped. Our readers did the most important part.

Dear *2600*:

I just wanted to thank VinceC (a *2600* reader tired of hearing the phrase "Free Kevin") for writing the letter that appeared in issue 17:1. This selfish moron who shunned the Kevin Mitnick case provided me with the hardest laugh I've had in months. Not only did this idiot give us a wonderful lesson on life (free of charge, no less), but to quote him exactly, "You fuck with the bull, you get the horns." I haven't heard that stupid ass saying since at least 1986! Thanks again to VinceC, the 80's reject, for the laugh.

Cowabunga dude.

Speedk0re

Fun With Cable Companies

Dear *2600*:

I get RoadRunner from Cox Communications, which is actually a pretty cool DHCP ISP, but what they did was stupid. They must have been monitoring my packets or something because I port scanned a friend from school. After a few days I noticed that I wasn't able to go online, so I called up Cox. They said I had some violation. The lady on the other end said I was trying to do a DoS attack on somebody and I was icmp flooding him. I tried to explain that a DoS attack would require many *many* more messages but they didn't believe me. They told me I was visiting sites like rootshell.com. I'm a freak about security (which is why I don't run NT) and was only trying to make my computer secure. What makes me really mad is that Cox is spying on its customers by looking at what sites they connect to! What business do they have over what site I connect to? Well, aside from having no Internet access for 14 days, I got in trouble with my parents and am going to have a hard time ever buying a *2600* again. Just thought you guys would like to know that.

RootX11

This is the risk involved when we hand over our Internet access to major corporations who dominate the industry. They can and do watch you and the sites you visit and have little or no understanding of anything other than their rigid policies. The obvious solution for you would be to switch to another company that understands what a port scan is and has some technical knowledge - maybe a site actually run by hackers. But how many people have the ability to choose one cable provider over another? How many non-Fortune 500 companies offer cable access?

Dear *2600*:

I read tacit's letter on BlackICE in the Spring 2000 issue and I just wanted to mention that this "firewall" seems to consider a ping to be an attack! My friend (who has a cable modem) has a copy of it, and I noticed he was receiving a lot of "attacks." I wondered how the hell anyone even knew his IP, since he never even does anything other than use the web. A couple of the "attacks" came from other Roadrunner IPs. I then noticed that most of them were "TCP probe attacks". Is that a ping or is it just me? Now pinging is considered a hack, I guess. Do we live in strange times or what?

jijack

Dear *2600*:

Snot Gnome wrote to ask about Cox Communications' channel 117, which contained what I think is a spectrum analyzer graph on it. I used to work at TCA Communications, the Internet branch of TCA Cable, which was just bought out by the much larger Cox Cable. I was the cable admin in charge of rolling out the cable system company-wide.

It is common practice to have a spectrum analyzer up at the cable headend to tell you what kind of interference is going on in a given segment at a particular time. And usually they'll have a little camera mounted up above it which is broadcast on a channel so that the field techs can go out into the field, adjust things, and then plug into a cable anywhere on the line, turn to channel whatever (117 in this case), and see if they did any good to help the noise.

So, Snot Gnome, if you want to know a trick that will not only tell you whether or not that is a spectrum analyzer on your node of the network, but will also disrupt everyone's TV and cable modem service on your node, try this:

Get a hairdryer, then get some coax that is plugged into the cable from the cable company. Then wrap the cable around the hairdryer several times. Finally, turn the hairdryer on.

What just happened: Since the cable you wrapped around the hairdryer has an open end, it functions as an antenna for your segment, and since you wrapped it around a moving motor, you created a lot of interference - basically broadcast a signal at *all* frequencies, overlapping all the specific frequencies that cable modems and TV signals come down and go up the cable line on. Now don't worry, you haven't permanently damaged anything, but for the duration of the time you run that motor in the hairdryer, you have disrupted the signal to all cable subscribers on your segment of cable.

This is the most annoying thing you can do to a cable company, especially if you do it a lot, because they will have to dispatch a whole team to sweep your segment to find the source. If you do it once or twice, they probably won't find you. But if for some reason you decide to do it on a regular and/or patterned basis and then you start seeing bunches of cable trucks in your area, you will know to stop because they are narrowing it down to your area.

I wouldn't suggest doing it on a regular basis because, believe it or not, even though cable companies are very stupid sometimes and provide crappy service, they really are concerned with providing better service. When you tie up their resources with something that is basically a stupid problem like this, you take their man hours away from real problems or doing things like rebuilding your backbone.

Rizzn Do'Urden

Info Needed

Dear *2600*:

I read an article in your magazine last year called "Hacking the Aspect." I found that information to be very useful when I wanted to set up a new idle code on my phone at work. Well, now that I have the Aspect switch down, my company has merged with another and we are getting a Lucent switch installed. Now I need to get information about that switch so I can begin having fun again. If anyone knows about them and would like to share, I would be grateful.

Popeye

School Update

Dear *2600*:

Yet another example of stupidity in schools: I downloaded a couple of the anti-MPAA leaflets from your site to post around my high school. It was a vain attempt, considering the type of people who go to my school, but I wanted to at least *do* something. I first asked my history teacher so as not to cause any problems. She thought it was an excellent show of political awareness and gave me the go-ahead. I posted them on a few different student bulletin boards around the school and left it at that. Big mistake. About three hours after I posted them, I got called down to the office. The principal immediately demanded to know if I had posted the leaflets. I said I had and he blew up. He threatened

me with suspension for "inciting students to illegal activities." Apparently, he thought supporting the side of the "DVD pirates" meant I was telling people to copy DVDs. He then asked me where I had gotten the leaflets from and I told him honestly. Another big mistake. He dragged me down to the computer lab and made me show him how to log on to both openDVD and your site. One look and he went nuts. He dragged me back to the office, started accusing me of being a cracker, and called my parents. He then carried out his threat of suspension and told me he would notify the authorities about my "obvious activities in computer crime." Turns out he didn't, but I was escorted out of the school by a security guard. I tried to explain the situation to my parents, telling them I only had posted a leaflet, but my principal got to them first. He convinced them to restrict my access to computers and search my room. He told them to restrict my access to phones as well, but they stopped short of that. When I was finally allowed back into school, I was prohibited from using the computer lab or pay phones. And the students decided I already was a criminal. They started blaming all the computer problems they ever had on me. Some even came straight up to me and begged me not to damage their computers. I wonder if I would've gotten this response if I simply put up a flyer saying "Save the rain forests."

Irubachi

And who says they don't teach you how screwed up our society is in school?

Dear *2600*:

With all the hoopla over hacker persecution and kids getting expelled for asking about Kevin Mitnick, perhaps I can point some things out. First of all, if you must take *2600* to school, try to keep it hidden. Although it may seem like bowing to pressure, it's much better than suspension or expulsion. Secondly, *keep away from your school's security programs!* If they happen to be running an incredibly vulnerable and loophole piece of software, print out a list of flaws and anonymously mail it to whoever is in charge of the computers. Don't get NetBunny or whatever. I did and am facing possible suspension. If you absolutely must put the latest and greatest s00p3r HaxOr program on the computers, *tell no one!* If you do, it will be abused and you will get to see the principal's office. Third, read the letters in *2600* and don't make the mistakes others wrote about. Life is as bad for the hacker who sticks his neck out as many letters report it to be.

Eric S.

Dear *2600*:

I've read the sad tales of other readers who have been condemned in their own schools for simply "exploring" the computers. I, however, am lucky. A week ago I was looking around the computers in the library and noticed somebody had installed the BO2K client on one of them. These computers being networked, I knew there was an immediate danger. I went through and deleted all files related to BO2K and searched the registry. At precisely that moment, the librarian came up to me and asked what I was doing. I told her I was fixing the computer (knowing her feeble mind couldn't comprehend what a favor I was doing). She panicked and went on about how I was "messing with" the files and, oh, get this, I was hacking, too! I was taken to the assistant principal's office where I was expecting two weeks suspension. Luckily, one of the techs the school contracts was in the next office fixing the PC there. I shouted from across the office hoping he would hear my cries for help. He came over and I told him the whole situation and exactly what I did and what I was accused of. He checked out the computer than came back with a smile on his face. He told them that I did nothing wrong. Then the librarian started telling the tech that I was hacking. He then stopped her and said, "No ma'am, he wasn't hacking, he was helping" and just started laughing. I urge other readers to take similar actions in trying get a respected voice to speak for them should this happen.

Code_WarriorX

If there were more respected and intelligent people hanging around, this would be easy.

Dear *2600*:

I wanted to add my input to P2129's letter in the Spring 2000 issue. We also have to wear the ID tags (I'm S6585). If you leave your ID at home, you must buy a new one for $5 or you have to leave. *Rip-off!* If you make a habit of forgetting this "dog chain," you could lose some good money or get expelled. It would seem to me that they (government) wants to turn everyone into robots with different serial numbers. Keep up the good work!

cs0074life

But it goes beyond that. Who is demanding these moronic policies? Who thinks the V-Chip and the Clipper Chip are the answers? Who wants to hand over virtually all responsibility to an outside force? We're living in an ultra-paranoid, suspicious society fueled by ignorance and intolerance. No government in the world would resist this enticement to take away some rights and help fuel the fear a bit. But ultimately it's the people who make the decisions, even though most of the time they don't even know they're doing it.

Dear *2600*:

Since everyone lately seems to be writing in with their own school story, I thought I'd write in with my own little interesting story. Mine doesn't involve me being mistreated a whole lot, well actually not much at all. I was a TA (Teacher's Assistant) last semester in the Counseling Center and had access to many computers in the center. One day when my "teacher" was off at a meeting the whole period, I decided to have a little fun with the computers. So I changed all of the desktop backgrounds. I went to 2600.com and changed every other computer to your logo with the dog and the guy on the top of your page, and on the other computers I tiled the little Free Kevin stickers in the background. The next day on the morning announcements it was announced that "someone has hacked all of the computers in the Counseling Center and this hacker will be caught." I just burst into laughter because of how stupid they were to say that their computers were hacked - all I did was simply change the background picture. What is the world coming to when schools are so stupid as to think that changing a background is hacking?

Blooder, The Tide on a strict leash

Dear *2600*:

Before I start, let it be known that I am an "old guy." I joined the ranks of the hackers via the phreaking route about 15 years ago. I am the "Internet Systems Manager" at a very large school corporation. We have (on any given day) somewhere between 15,000 and 20,000 students in attendance.

Firstly, I have so little respect for academia now that I work for a branch of it that I am considering home schooling my kids. I have worked for this K-12 school corporation for six years. What I see is a preponderance of techno-ignorance the size of which would beggar your imagination. But yet, these people know that if they don't have the toys around, they will be looked down upon by the community. So, begrudgingly, they are trying their best (which ain't so good) to use the technology. Don't get me wrong, there are some who are masters at both teaching and technology. But to most of them, it's just a job. To those who talk the talk and walk the walk, I salute you!

Budding hackers: Fear not the wrath of your teachers and administrators for they know not what you do! So when they haul you to the office or question you, don't smart off. Just be quiet and respectful. When they are done yapping about this and that, ask them these questions: What evidence do you have that I was hacking? If someone was hacking, how would you know? Why is hacking bad and why are hackers bad? Do you know the difference between a hacker and a vandal? What are the moral implications of hacking as opposed to falsely accusing someone of something when you have no evidence or idea of how it would be accomplished?

Someday soon I would like to come up with a strategy for budding hackers to follow. But for now guys. Do No Harm, Leave No Tracks, Be Respectful. I find that you can accomplish more by asking respectful questions that help the people who are accusing you realize how stupid they look and sound.

ICMP

Criticisms

Dear *2600*:

I am a new subscriber (today really), and I was reading your Winter 1999-1900 (nice touch btw), and saw an advertisement for boycotting Brazilian products (more specifically coffee). After visiting the web site for the campaign, I noticed that it sounded a lot like *X-Files* where the U.S. government is trying to implement some sort of mind control program. The crux of the whole issue is that Brazil is the main site for their experiments.

Personally, I have two problems with that. The first is that I am a Brazilian and know quite a few people in power there. They tell me many things that go on down there, but when I questioned them about this program they told me they had no clue about this. I know that this is probably the standard answer about all programs that are run in "secret," but they have no reason to lie to me. Also, they mentioned that should Brazil be participating in such an "experiment" and the truth was discovered, they would have too much to lose with some of the US's enemies who are active importers of Brazilian products. Second, the Brazilian government doesn't have the facilities with which to do such an experiment. They are more interested in lining their own pockets. They would never spend enough money to finance something this big.

I understand that *2600* is a strong supporter of freedom of speech (which I endorse), but that should not include outright lies, which is what this Boycott Brazil campaign is based on. There is another side to that story, which you should consider when publishing future advertisements for that campaign.

Patrick

To start with, we take no position either way on Marketplace advertisements our subscribers place. The only time we take an active interest is if it's a rip-off of some sort. Now, as for the assurances you received from the people in power down there, surely you don't believe them just because they said so? If you really want to get to the bottom of this, do everything in your power to prove that it's true. That's the only way you can conclusively prove that it isn't.

Dear *2600*:

I am terribly sorry about the irrationality of the MPAA. However, I can't quite figure out why you would print articles dealing with United States government security. I am referring to two articles in the latest issue. I mean the last thing you need is the federal government on your trail. And there is an ad stating that someone will fax secrets of the White House Communications Agency. Why would you print such a thing? And don't tell me its because he's a subscriber. I am so proud to read your magazine but would hate for you to go down in flames over something so stupid.

cryptofreq

We talk about government security because it's of interest. If we were to self-censor our material because we were worried about what someone might think, we wouldn't be able to print much of anything. Concerning the ad, it's interesting that you inserted the word "secrets" into it. The original ad never said that - it simply offered "documents" that are most likely public but not easily found. This is exactly our point - if we followed your advice, we would have turned the reference material into a secret and not printed the ad even though we had no evidence. Our fear would have silenced us long before any action from a third party. We can't go down that road. Comfort yourself by knowing that anyone foolish enough to trade classified info through our Marketplace will certainly get an unwanted letter very quickly.

Continued on page 48

Continued from page 5

music over the net is just not the same thing. In all likelihood, more people will be exposed to new artists as a result, meaning the record companies will no longer be the only way they can reach the public. This obviously works much better with artists who are looking for exposure on the net. Those who don't want their material spread in this way should make their wishes known, but we cannot see how, short of banning anonymity altogether, it would be at all possible to prevent people from trading music.

Such thoughts are not at all far from the controversy. In recent remarks at a conference, Edgar Bronfman, chairman of Seagram, which owns Universal, which, yes, is suing us under the DMCA, came up with this gem: "Anonymity... means being able to get away with stealing, or hacking, or disseminating illegal material on the Internet - and presuming the right that nobody should know who you are. There is no such right. This is nothing more than the digital equivalent of putting on a ski mask when you rob a bank." Make no mistake - anonymity is as much a perceived threat to corporate America as encryption has been to the Clinton administration. In both instances, the very fabric that defines the net is being remodeled by people who have no right at all to do this. Unless we let them.

And then there's speech. Free speech has always been the enemy of those seeking to exert massive control. Now that legislation has made it possible for this control to be extended to the net, we can look forward to increasing attacks on mere speech. For instance, if you intend to register a domain name that is critical of a corporation, watch out!

It used to be that you could criticize whoever you wanted and, as long as you weren't libelous, your rights were respected. That's all changing. George W. Bush said it best when he tried to shut down www.gwbush.com for being critical of him: "There ought to be limits to freedom." Fortunately, he failed. But many others are continuing to attack speech nonetheless.

In addition to some parody political sites of our own, we thought it would be fun to register a few four-letter word domains as well - this became possible within the last year as Network Solutions stopped being the only Internet registrar in this country. For years, they had prevented the use of certain words because they considered them offensive. Now, thanks to competition, you can find a registrar who will give you the site you want. And that's how www.fucknbc.com was born. We didn't even get around to publicizing the site or, for that matter, making a site. We simply pointed it to NBC until we could figure out what to do with it. Somehow, the folks at NBC found our domain name and threatened us with legal action if we didn't stop engaging in "trademark infringement." They either honestly believed that by having NBC anywhere within the web site's name that we were somehow violating their rights or they think they have the right to tell us not to point our sites at them. Neither of these assumptions is true although we have started to see challenges on many fronts recently concerning linking from one site to another. The MPAA has tried to get us to remove our links to other sites which still have the DeCSS files by filing even more court papers against us. This time, major media not owned by the corporations suing us such as the *New York Times* made a point of linking to our links to show their opposition to this motion.

The fun continues with a company that technically doesn't even exist yet. You may have seen some advertisements for Verizon Wireless, who have somehow managed to co-opt the peace sign as their corporate logo. That's just the beginning - a really big company will be named simply Verizon and it is set to encompass all that is currently Bell Atlantic and GTE. In an effort to stave off those free speech advocates, at least 706 domains were registered, including all variations of

verizonsucks, verizonblows, verizonshits, you name it. Apparently, their new logic leads them to conclude that if they simply take all of the critical names, nobody will be able to criticize them. So we decided to take www.verizonREALLYsucks.com, knowing that we would one day find a use for it. It didn't take long. This time the legal threat said we were violating the new anti-cybersquatting law and that we were required to immediately hand over the domain to them for free. While some of the goals behind the anti-cybersquatting act were worthwhile (people who take a company name for the sole purpose of selling it to them at a huge profit are rather sleazy, after all), we knew it would be quickly abused. There is nothing even remotely related to cybersquatting in what we have done. Verizon obviously has all of the sites it wanted to register. We simply thought of a new one that criticizes them. Since they already took sites that criticize them and obviously have no intention of using them for that purpose, they are a lot closer to cybersquatting than we are. While we're pleased that we may be Verizon's very first lawsuit, we're annoyed at the utter waste of time these huge entities continue to cause.

We have a distinct advantage as we're able to tell the world when things like the above happen. But there are countless other cases going on right now where individuals are being targeted because some corporation with a huge legal team doesn't like something about someone's site. How likely is it that an individual will be able to stand up to this? Not very, if we don't stand up for each other.

Our trial has been scheduled for Monday, July 17 (the day after the H2K conference ends) at the Federal Courthouse in New York. We hope to see many of you there. Check www.2600.com for updates and any changes.

A SIMPLE HEX HACK

by Zarathustra

This is a pretty simple spoof on a date value stored in the registry and is written as simply as possible which is a pretty weak hack, but when I was just getting into the scene, I would have loved to have found an article like this, partially as a good example of how to proceed, but mostly as a confidence booster. Doing the hack yourself makes you understand what's actually going on and gives you the confidence that you can succeed. The key is that it's so simple to do that you don't need to understand assembly language or how the V-Table is set up, nor do you need any specialized software so there are no roadblocks to keep you from doing this.

Hex Workshop's Registry Based "Security"

Hex Workshop is a hex-editing program for Windows 95 from BreakPoint software. When I downloaded the trial version of Hex workshop V2.54 (not the newest one because it can fit on a floppy), and installed it (no EDIBC support), it told me that I have a 90 day trial edition of this software. Fair enough. The next time I ran it, five seconds later, it told me that I had used up my ninety day trial, and that I had 14 days to register. Next, it told me that I have totally expired my trial and that I had to buy the software. This really raised my interest as to how this product was calculating time, and so, assuming that my clock being set to May 11, 1980 was a root of the problem, I started to investigate.

Hex Workshop has two different security mechanisms built in: the first one is so that you can insert your serial number in order to enable the full version, and the second is to disable the product once you've used it for more than ninety days. This article focuses on the second. The great thing about cracking non-network enabled software is that you have the entire puzzle in front of you, and all you have to do is understand what's happening. If you don't understand what's going on you have no hope of ever cracking it. Because this program is time limited, it must have a date stored somewhere. If you can find where the date is stored and how, you'll be a lot more successful modifying that than trying to directly modify code. Good targets are small, suspicious files in the program directory and the windows registry. In this case, running regedit, and looking at "My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\BreakPoint\Hex Workshop\2.50" reveals the keys "Major" and "Minor". Taking a wild guess, I erased them, then ran Hex Workshop which told me that this was the first time I had run the product. Bingo! The next time I ran Hex Workshop, it told me that I had fourteen days left to register and the next time it told me that I had used up all of my time. This was obviously the pertinent data. It was starting to look like there wouldn't too many pieces to this puzzle.

After much experimentation with changing the windows system date and seeing the effect on the keys, I learned that:

The Minor key had to do with what step of the security process you were at:

Minor value	Means
00000000	Still free.
AA000000	14 days left to register.
BB000000	Locked out!

When the program hit the 14 day point, it changed the Major key, which I ended up never bothering to explore. If the date is set to before January 1, 1990 then running Hex Workshop advanced the minor value by one each time. If the date is set to after Jan 18, 2038 then Hex Workshop crashed every time. Advancing the date by one decremented the fourth bit by one. Advancing the month by one decremented the second bit by one. Advancing the year by one decremented the last bit by one. Deciphering what I assumed would be an encrypted date was starting to look a lot simpler that I had thought.

Okay, so here's the Major Key formula:

MMDDYYYY					
YYYY	MEANS	DD	MEANS	MM	MEANS
F843	1981?	E0	31	FB	JAN
F842	1981	E1	30	FA	FEB
F841	1982	E2	29	F9	MAR
				F8	APR
F839	1980	EF	18	F8	JUN
				F7	SEP
				FE	OCT
F810	2037	FD	02	FD	NOV
F809	2038	FE	01	FC	DEC

Which means that date and month are FF(hex) minus the MM or DD, then converted to decimal, and year is FFFF-DDDD converted to decimal. Other than the sneaky month thing this could be a windows default encoding.

Although one could easily write a program to write yesterday's date to the "Major" value using RegOpenKeyEx, it turns out that writing "000AAAAA" to the Major key and 0 to the minor will always avoid the date check problem. Unfortunately, it doesn't stop the program from crashing after January 18, 2038 or from resetting the registry values if used before January 1, but in order to fix that we'd have to debug other people's code, which is beyond the scope of this article.

I hope that this was an interesting introduction to the exciting world of cracking software. Although this was definitely beginner level and most projects are a lot more complicated, the same basic techniques can be applied to a lot of software. The key is to be able to recognize when to switch from modifying data to modifying code. With an increasing emphasis on modular software development, software tends to have lower cohesion, making it way easier to modify with no side effects. With super-high pressure on programmers, a lot of shoddy code gets released. So if a product has encrypted data you might as well check the binaries for security holes. In addition, you'll find that as you trace through more software, you'll develop a greater appreciation for why and how Windows works.

SECRETS OF DELL

by Deamtime

I work as tech support for Dell computers. Because of Dell's reputation and tradition for reliability and technical excellence, we recently became the biggest OEM, both domestically and internationally. Because of this fact I thought a brief article about this brand of computer might be in order.

Same Computer, Different Support

The first thing you ought to know about Dell tech support is its divisions. All accounts fall into one of three categories: HSB (home and small business), PAI (public and international), and Relationship (large company accounts). Different divisions have different support policies and boundaries. Most computers are in the HSB category. Computers in this category have a "magic 30 day" window from their ship date. PAI accounts are mostly government and education accounts. I haven't had any experience with the Relationship accounts so I won't talk about them.

General Dell Info

All Dell BIOS chips are branded with the computer's service tag. Service tags are five digit (some new computers have seven digit tags) alphanumeric identifiers of the specific computer. The database lists all of the information about the components and software that the computer shipped with. It also lists most of the owner's information, including the credit card info. This database is a simple SQL database with laughable security. It also, until recently, has been run off of Compaq Tandem servers. Go figure. The service tag is imprinted into the BIOS for the purpose of identification in the case that the computer is stolen. It can also be found on a sticker on the case.

Dell, like most major OEMs, purchases special versions of most system components. If you see, for instance, an advertisement for an SB Live! card and order one for your Dell the features are likely to be different. Also, many of the cards now have an EPROM chip on them that records the last time diags were run and the results. I don't know how much storage is on the chips or what else they may record, but it isn't unlikely that they store information about the operating system, configuration, or any of a host of other "diagnostic" information types.

The "Magic 30 days"

For HSB computers the first 30 days after they ship they are under a "total satisfaction" warranty. My advice is that anything you are likely to do with the computer, do within the first 30 days. If you are going to install Linux on the box, do it then so that if you are unable to tune any specific driver to your liking (or even if you end up damaging components with "risky" code) you can get a replacement for that component or even for the full system. During this time you can also get upgrades to most components at cost. (This means "really cheap.")

After this 30-day period most computers are covered by a year's worth of "onsite" warranty (although you can also purchase two additional years of this warranty). If you don't want some stranger coming over to your house and fiddling around in your system (not a bad choice, from what I've seen of their work), you have the option of replacing the part yourself. If you take this option you will be asked for "collateral information" which is generally your credit card info. If you refuse to give it to the tech, they will have to get manager approval to send out the part anyway (generally, this is pretty easy to do). The reason for the collateral info is that Dell almost always wants the defective part to be shipped back to them. This aids in issue tracking and also allows for refurbishing. Almost all parts sent out in this manner will be refurbished. You can request that new parts be sent to you (this also requires an approval, which will almost never be granted if there is no collateral info). I've seen this become an issue most often with monitors, which go through almost no testing before being reissued.

The next two years generally are "parts only" service. This service follows along the lines of the above requested self-install.

Classified Drives

PAI accounts differ from HSB accounts in several ways. First off, PAI customers do not have to troubleshoot over the phone. They also have the option of "classified drives." A classified hard drive is one that is suspected to contain sensitive information. These drives are most often in the Department of Defense, although any PAI customer may claim one. There is no record on the service tag which computers have classified drives. These drives, when defective, are destroyed on site and are not returned to Dell. You have to inform the technician that you have a classified drive, as they will not ask.

ZZTop

All Dimension computers come with a compressed drive image on a hidden partition. The only certain way of absolutely getting rid of this partition is a low level format. This "hidden" partition isn't a partition at all. The image is written at the end of the drive. The executable program "ZZTop" finds, expands, and writes this information to the drive, much like Norton's "Ghost" program. Many images are coming out of the factory corrupt these days (see the "Dell Today" section below). If this is the case and it is discovered within the first 30 days, you have the option for an STM CD. This CD contains the same information. If you decide to use the STM as a system maintenance utility, make backups of both the CD and the floppy that comes with it. If either one fails past the first use you will not only get no sympathy but no replacement.

support.dell.com

All technical information, from pin-outs to jumper settings, white papers to driver files, on all Dell components ever shipped (including 8086's - seriously) can be found at the support web site. The search function is a little sketchy but with a bit of persistence you can find any information that you might need.

SE Tech Support

"Acts of God" are not covered under the HSB warranty. If a lightning storm took out your modem, for the love of all that is good don't tell the technician. As soon as that is entered into your log, that part cannot be replaced by any technician. All phone techs have a badge number to identify them. Make certain you get that number and use it whenever referring to the tech in your communications with Dell. All branches of support have five digit extensions to their queue. Get that number and watch your call times plummet. Don't mention that you are taping a call - you will be hung up on immediately. Don't threaten legal action - your tech support will be suspended completely until the legal department reopens it. (Only method of contact with legal? Surface mail, naturally.) Also, don't just stop making payments on your computer expecting that Dell will repossess it. Instead, they will take you to court, usually filing in a federal court (interstate commerce) in North Dakota or Hawaii on a Wednesday. They give minimum notice, usually down to the minute and almost always win. I have heard that they are able to garnish wages and totally destroy credit for years.

Dell Today

Redhat has started shipping on some Dimension desktops. Support is by Linux Care.

The Dimension line seems to be plagued by unreliable modems. Do not under any circumstances order any Conexiant modem on a Dimension. Dell has terminated their contract with Conexiant and will stop shipping their POS when they run out of stock. I have seen examples where a customer ordered a USR hardware modem and got a Conexiant instead. Read your invoice carefully. If this happens to you, call customer service. Because of the increase in sales, the computers are not being burned in any longer at the factory. I have seen instances that make me doubt that they have even been turned on. Loose or unseated cards are not uncommon (sometimes even processor or ram). Neither are unconnected power or data cables. Misinstallations of software and poor backup images are also common issues. Burn in your computer when you first get it.

This article didn't mention anything about laptop or server support. I don't know much about those divisions. All I can guess is that they are much the same as we are. Have fun with your Dell and, hey, have fun with Dell too!

HOW DOMAINS ARE STOLEN

by Crim, Redomega

Network Solutions controls many of the .com, .net, and .org domain names for the Internet. When you purchase a domain name, you are expected to supply them with three contacts for your domain: Administrative, Technical, and Billing. You are also supposed to supply each contact's name, address, phone number, and e-mail address. All of this information is kept in NSI's public Whois database (www.networksolutions.com/cgi-bin/whois/whois).

Modifying a Domain

So you've registered your domain name with NSI, but you need to modify or update your contacts or name server address. You simply go to www.networksolutions.com/makechanges/ and supply it with your domain name. Fill out a Host Form for your domain and use the "Mail-From" authentication. This will e-mail you the correct form to update your domain. When you receive this form in your e-mail box, you are supposed to send it back to hostmaster@internic.net and it will check your e-mail address with the one in its database to see if they match. If they do, your domain is updated.

Exploiting

Updating NSI's records using the "Mail-From" method doesn't seem to be all too secure. The easiest way I have found to modify someone else's domain is to request a modify form from Network Solutions and save it to your hard drive. From this you can change form blanks to whichever domain you wish to modify. After making your changes to your form, the only problem is having the e-mail sent from the technical contact's e-mail address. This is easy to do. Look up the technical contact's address using the above Whois database. Then you can use a somewhat well known trick to "spoof" your e-mail address:

1. Telnet into any mail server on port 25: telnet mail server.com 25
2. You should connect to the server's SMTP server. You need to give it false info by entering: *HELO some.fake.website*
3. Now to tell the server who is sending the e-mail, put in the technical contact's e-mail address: *MAIL FROM: address@server.com*
4. Now that the SMTP server knows who is sending the E-mail, you need to tell the server to whom the e-mail is being sent to. Put in: *RCPT TO: hostmaster@internic.net*
5. Now tell the server to start the body of the e-mail: *DATA*
6. Now you should paste your domain modify form into the telnet session.
7. To send the e-mail type a period on an empty line.
8. Then type *QUIT*

This will send hostmaster@internic.net the domain modification form as if it came from the technical contact's e-mail address, and it will process the form. The only problem I see in this method, is that hostermaster@internic.net sends out two automatic e-mails to the technical contact's address. The first is just an acknowledgement that it received the form and the second shows that the changes have been made to the internic database.

Playing With Dominos

by Dr.Clue
dr.clue@grond.demon.co.uk

Lotus Notes/Domino is a groupware system, essentially allowing easy sharing of information between people. It's a client/server system, composed of the Domino server and the Notes client. It's big. It's complex, and it's got an awful lot of things that don't quite make sense when compared to other environments. This makes it a challenge to learn, but also means there's a lot of confused Notes admins out there!

There's no way I can cover everything here, but I'll try and concentrate on some of the main ways to have fun with Domino.

Notes was developed by a subsidiary of Lotus, called IRIS Associates. They have a help site called notes.net, where you can download upgrades, trial versions, and moderately useful documentation.

Basic Concepts

Notes works with documents. Within a database, you have forms which documents are created from. They define the fields, layout, and any scripts that are executed. Once documents are created from forms, they are viewed and organized by views. You can also create folders, that function like views, but contain copies of the document. So a document can be seen in more than one view, but it is the same document - delete it from one view, you delete it from the database. A document in a folder is a copy that exists within the folder - delete it from there, and it will still be in a view somewhere within that database. OK? Let's carry on, then.

Poking Around With the SMTP MTA

Let's start by looking at Notes mail. The Domino server has a Public Name and Address Book (PNAB) which contains all the users for the Notes domain, plus all the groups. Additionally, people may have defined extra groups in their local NABs, but these are obviously only accessible to them within their own Notes client. The Notes domain is essentially defined by the PNAB.

When sending email within Notes, all you're doing is just replicating a document between servers - it's not a mail system in the "real" sense of the word. This has some interesting side effects for us - firstly with the SMTP MTA. This is an add-in task running on the Domino server which converts the Notes proprietary mails into SMTP, and vice versa. With Domino 4.6 and earlier, most of the anti-spam and anti relaying features were adding as statements to the main notes.ini file. These statements are cryptic, and many lazy admins haven't bothered with them.

As SMTP isn't native to Domino, it must convert incoming email from SMTP before it can apply any restrictions. This gives us our first DOS. If you send multiple emails into a Domino server, it must accept them and then convert them fully. Once converted, Domino checks its notes.ini file to see if it should bounce those emails. If it should, it either converts the email to SMTP again and bounces it, or else forms a Notes NDR report, converts that to SMTP, and sends that back.

As you can see, the Domino server is doing a ton of extra work here - just flooding it with emails that it must reject will bring the server to its knees. However, that's a bit lame, so what else can we do? Well, Notes uses an X.500 like hierarchy of certified IDs - like Joe User/Development/ACME. This gets converted and spat out the SMTP MTA, depending on its config. Using the above example, the Notes internal mail address would be:

Joe User/Development/ACME@ACME

and the most common SMTP equivalent would be:

joe_user/development/acme.acme@smtpmta.domain.tld

Often the SMTP MTA is reconfigured to show:

joe_user/acme@smtpmta.domain.tld

Using this addressing scheme, and with a little trial and error, you can bounce messages through the MTA to internal Notes groups. Bounce messages and SMTP errors are logged into the standard Notes log on the Domino server. This is crowded and difficult to read. An enterprising Domino admin will create special views within his log to view certain MTA events. However, because the MTA is essentially an add-in, your options here as an admin are limited. This means there's quite a high chance your poking around will go unnoticed. Certainly, it can be followed through that if an admin hasn't secured his MTA against relaying, he's unlikely to have gone to the effort of creating special views to check on the MTA's activity.

Via the Web

Domino servers also have an add-in http task. When Notes 4.5 came out, this add-in was called Domino. Version 1 and 1.5 were launched, before the marketroids confused the whole scene by changing the name of the Notes server to Domino. From 4.6 onwards, http has been bundled as an add-in, as well as other interesting things like NNTP and the SMTP MTA. One of the first things any competent Notes admin will have done is disabled database browsing. If they haven't, when you connect to the Domino server, you'll see a nice listing of all the databases on the server with their directory structure. Nice. Accessing a Notes database via a web browser is easy. By default, the http task will add a "?Open" to the end of a URL. So, for accessing the Notes log, we would use:

http://domino.domain.tld/log.nsf?Open

There's a host of "?" commands that can be used. "?EditDocument" is always handy. "?OpenForm" is also nice. Have a dig around and see what else you can come up with.

A Word About ACLs

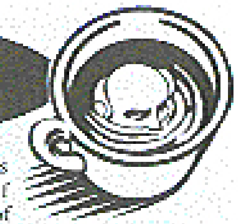
Access to the Notes database is configured by ACLs - the two most important entered being Default and Anonymous. Default is on the ACL by, well, default - it defines the highest level of access a user is given. This is overridden by either specifically mentioning the user in the ACL, or by using a Group with them as a member. Anonymous is not on the ACL by default - this defines the highest level of access available to a non-authenticated user. There is also a switch defined in a separate area of the ACL called Maximum Internet Browser Access. By default, this is set to Editor, which means you can create documents, and edit and delete other people's documents. Lotus doesn't, by default, ship very secure ACLs for the standard databases. This is getting better with R5, but the admin still has to go through his databases manually and configure secure ACLs. This tends to mean that some databases slip through, with Default access giving more than it should.

Domino Logging

The Domino log database is called, quite originally, log.nsf. This is where things get stuffed and where an alert admin will look to see who's been playing around on his servers. Access violations (and other errors like File Not Found) will also appear on the Domino server's console. The http task can be configured to either log to the Notes log or else to text files living in the data directory. Domino will log separate files, making it a pain to use standard log analysis tools (which expect one file in CLF format). The main ones are access log, error log, and referrer log. Databases themselves track user accesses, and what you do. You can only delete this from a Notes client and if you have Manager access to the database. However, if you haven't authenticated, then you will appear as Anonymous on the list. So to track you down, the admin has to search and synchronize entries in the database's user activity list, the Notes log, and the http access and referrer logs. Bit of a pain, eh?

I hope this has given you a bit of an insight into Domino, and has whetted your appetite for more. Have fun and explore, but don't be destructive!

Java Applet Hacking



by Xprotocol

When you go to check your e-mail, you type in your name and password and, if correct, you get access to your mail. E-mail websites use what is known as CGI programs. These are programs stored on an e-mail server used for many things like password prompts, online polls, etc. The only way to hack a CGI program is either by brute forcing someone's name or gaining illegal access to the server and searching for password files.

Many people have a non-virtual domain website (meaning they don't get a .com but something like www.geocities.com/area51/nebula/1416/) which they probably get for free. The server may not offer CGI tools or even a CGI bin to store your own programs. Even if the server has a CGI bin for your programs, you still need to know the language. However, many websites and servers offer free Java Applet source code for neat webpage design. Someone can easily get ahold of this code and put a password prompt on their website for friends or members. Since Java is a program about as much as HTML is, it can't be used for high security. Any password prompt that is a Java Applet just takes you to another site. Example: You get a Java Applet prompt at www.awebsite.com. Entering the correct username and/or password will take you to www.awebsite.com/home.html. Someone could easily guess this and go directly to the so called protected website with no password prompt. However, if you try this with a CGI script you will get an "Incorrect name or password" message or a username and password prompt.

As you can see, Java is the much easier choice, but comes with less protection. Many non-virtual domain websites will use Java Applets as a source of security. The neat thing for hackers is that these can be hacked very easily and without having to gain illegal access to that server. When I first came in contact with one of these things, I had no Java experience at all and very little programming knowledge. I broke through the barrier in about two days.

First, you may want to install an HTML editing utility such as Frontpage Express. If you can't get ahold of one, using Notepad will work just fine.

Find the password prompt that you want to break. Make sure that it is Java. At the bottom of your browser there should be a message that says "Applet Initialized." This means that the password prompt is Java. Using Internet Explorer, right-click on the page and choose edit or view source if you don't have an HTML editor.

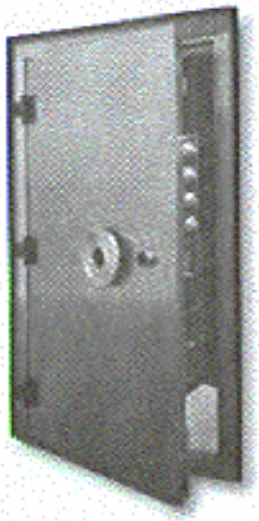
In the editor, it displays the Applet as pasw1.class. In Notepad I get the entire HTML code with a string that looks like this:

<applet code="psw1.class" align="baseline" width="367" height="187" archive="psw1.jar">

This tells me that the Applet uses two sources of code, psw1.class and psw1.jar. Psw1.class however is just the Applet code and is contained within the HTML of www.awebsite.com. Using Internet Explorer, I type in www.awebsite.com/psw1.jar. This asks me if I want to download or open the file. Select open and choose Notepad when asked what to open the file with. I search through all the code looking for a file. I find one we'll call text.txt. Using IE again, I type in www.awebsite.com/text.txt. There in front of me is a list of usernames and passwords. I can now use these to determine the hidden webpage. I type one in and it takes me to www.awebpage.com/home.html. I can now type directly into my browser this address without getting a password prompt.

Right now you might be wondering, "If I'm not breaking into the server and just going to a public website, is this illegal?" Well, yes and no, but no for the most part. The person might not be able to sue you because he did not use strong enough protection. However, you might not want to take the chance. If you really want to do this, go ahead and do it on a public computer.

The technique to breaking Java Applet passwords is looking through all files associated with that page and looking for more until you get some sort of list.



by obitus
(obitus@marmoset.net)

The purpose of this box is to add a measure of privacy to your phone calls. It does this by blocking your phone when someone else in the house picks up another phone on the same extension.

Theory/Background

This box is based on the Fuscia Box that was included in *Hacker's Information Report* #2. I was not able to get that box working so I set out to make my own, simpler version. Basically this is the theory behind the device: your phone line has electricity running through it. When you are talking to someone, the voltage is around 20 or so volts. When someone picks up another phone in the house, the voltage is cut in half. The box runs on two 15v zener diodes. The diodes only allow the electricity to flow through it if it is above the preset voltage of the diode. So when there are two phones in the house off the hook, the voltage on the line is only like 10 volts. That isn't enough to flow through the diodes, which causes your phone to be blocked. You have to use two zeners because, depending on how you have the box hooked up, the electricity flows through differently. With only one zener, the box would only work 50 percent of the time because the zener only tests the voltage if the electricity is flowing through it from a certain direction. From the other direction, the electricity can flow through freely.

Construction

The first thing you want to do is run over to your local Radio Shack and pick up a few things. Here's what you need:

1 modular phone jack.
2 15v zener diodes (they come in a two-pack).
1 small switch, such as an spst micromini toggle switch (the type really doesn't matter - you just want it small enough to fit in the phone jack). You will also need a couple of feet of phone cord.

Assembly

1. Open everything up and spread it out on a clean workbench. You will want a screwdriver, something to strip wires with, and these directions close at hand.
2. Locate your modular phone jack and open it up. Inside should be eight screws with eight wires running to them. The two that we are working with are the red and the green.
3. Unscrew the other screws. You may want to keep the black and the yellow wires. Cut the rest as close to the socket as you can.
4. You should have a red wire and a green wire running from the socket to two separate screws and six empty holes.
5. Move the green wire and screw it into an empty hole.
6. Next, solder two short wires to the poles on your switch.
7. Then solder the two anode ends of the two zener diodes. (The anode end of the zener is the end not marked with a black stripe - look at the back of the package that they came in.)
8. Take your phone cord and cut off one of the plugs. Peel back the insulation and expose the green and red wires. Strip the ends of these wires.
9. You will want to screw the red wire from your piece of phone cord to the screw that is holding the red wire from the socket.
10. Next you will want to screw the green wire from your phone cord to the screw that isn't holding anything at the moment. One wire from the switch and the cathode from one of the zener diodes will also be screwed to that screw.
11. The other wire from the switch and the cathode of the other zener will be screwed to the screw that is holding the green wire from the socket.
12. Lastly, drill a hole in the cover of the modular jack and push the switch through. The cover should just snap on.

That was easy, wasn't it?

Use

To use this sucker, just hook it between the wall and the phone. You will have to figure out which way is "privacy mode" and which way is "bypass mode" if you used the toggle switch. To do this, call up a friend and tell them to chill for a second. Flip the switch back and forth. You should be able to talk to your friend with the switch in either position. Next, run and take another phone off the hook in the house. Run back to the phone with the box connected to it. Flip the switch back and forth. In one position of the switch, you should be able to talk to your friend. This is "bypass mode." A flip of the switch should yield a dead phone. This is your "privacy mode."

Conclusion

This is a pretty easy box to build. There is a limited amount of soldering involved, so even the novice phreak should be able to build one. As I said before, the concept of this box is based on the Fuscia Box article in *HiR2*. I just simplified the design a bit. I have found that these modular phone jacks are useful for building boxes in. They are fairly small and portable. They can be used to add features to almost any phone. If you screwed some wires with gator clips attached to them to the same screws that the piece of phone cord is screwed to, you could make a beige box that would block your phone if the line you were trying to phreak was in use.

Continued from page 38

Dear 2600:

While in many cases you do the ethically correct thing by discouraging miscreants who would only disgrace hackers further, in some cases, you fail to gracefully admit when you are wrong (case in point: om's letter in 17:1). It is the mark of a mature and responsible individual to admit their faults, and you do not seem to be able to do so. Aside from this minor complaint, you are doing an excellent job of spreading the hacker message, and opposing forces of injustice everywhere.

You can write one of your snide responses to this letter about how om was the party at fault in your exchange, but his point about the contrast between user and administrator is a valid one, a point which you refuse to acknowledge.

The_36th_Chamber

Actually, we did acknowledge that Geocities had the right to remove pages of people who got around the ads. We're not disputing the existence of the contract. But we find the premise of the contract to be morally repugnant and something that users will (and should) try to bypass. Technically we're all supposed to be watching the commercials on TV but many of us fast forward through them. We maintain that any time one is forced to endure an advertisement, it is wrong.

Dear 2600:

Being a firm believer that someone should construct their own computer anyway (sort of like tying your own fishing flies), I was mildly offended to have found such a stupid article in 2600. First of all, the cost for building your own machine generally comes out as being more for a couple of reasons (most notably geeky pride and the search for more 31337 parts), but you get exactly what you want in a machine. Secondly, who the hell would want three ISA slots? Thirdly, "Don't buy Intel." Riiiight, why would I want a good chip when I could buy an AMD chip. Fourth, "768 RAM"??? Bober wants to put three 256mb chips in there?! You most likely wouldn't need a keyboard or a mouse with that setup because it would cost both of your arms and a leg to get the RAM. I do have to say thanks to Bober for pointing out my error - I guess I had always pronounced SCSI as "scuzy" when, in fact, it should have been "suczy."

dustbert

Helping New People

Dear 2600:

In 17:1, phiber_life wrote in talking about people on IRC who refuse to help out neophytes coming around, asking questions. I am one such person, for a few reasons.

First, I'm on IRC to chat with my friends. If I were in #please-ask-me-all-your-hacking-questions I would understand. But I am not. I never promised any information and people insisting on bothering me when I tell them I'm busy are not people who deserve my respect.

Second, almost all of the questions are either "How do you hack hotmail?" or "Can somebody teach me how to hack?" If you try and explain that it's not a simple matter of pressing a button like in *The Net* they lose interest. So why should I bother with someone who doesn't really want to learn?

Notmyrealhandle

If the name of the channel you're in is some how appealing to people who want to be part of the scene, you should consider that when you're deluged with questions. If you simply want to talk to your friends, IRC enables you to do that completely unseen if you so choose. It's also a trivial matter to set your client to ignore anything an idiot says. What's most important is that you don't judge people asking questions as morons until they do something that proves they deserve the label. Perhaps there are some IRC users who wouldn't mind the designation of "stupid question answerer" and who wouldn't mind when the rest of us transferred these people over to them.

Ideas

Dear 2600:

I have an idea on how you guys can get more subscribers. Make it so that when you subscribe to *2600* you get a piece of gum in each issue that you receive. Wait, make that a pack of gum since this is a quarterly mag. This way, even if people aren't pleased with the quality of the mag, at least they have a pack of gum, right?

Me and my friend did this when we made our parody mag *Random Acts of Stupidity* and we found that the general feeling was that people enjoyed the gum (a mag and a stick of gum for $1.50, wow!). Although we got suspended for our views in the mag, it was a great success. I think the gum deserves the credit for this one though. Anyway, just an idea.

MrBid

Everyone enjoys gum - there is no doubt about that. But we feel we should stay focused on what we do best and stuffing thousands of packs of gum into envelopes ain't it. Since your views managed to get you suspended, they must be worth something. We hope you pursue them and leave the gum for your teachers to hand out.

Injustices

Dear 2600:

When I was boarding a flight in New Jersey, after I had put my bag through the X-ray machine, I was pulled aside. The security guard decided to do a random search through my bag (which I had absolutely no problem with). As he was searching, he found a *2600* magazine and immediately confiscated it. I asked why he did this. He responded, and I quote, "I don't want you hacking into the airplane's computer system and crashing it." I laughed when he said this and walked away.

Is this world so uneducated on the meaning of real hacking? Don't people know that the real hackers hack to gain knowledge and not to cause destruction? I was appalled by this!

My story continues. As I was boarding the airplane, the security guard had two other security guards waiting for me. They immediately pulled me aside and began to question me. After all was said and done, they took away all my electronic devices (CD player, electric toothbrush, Gameboy, etc.) fearing that I would hack into the airplane's computer. I really think people should realize that to hack something you *must* have a system with an input and output device a.k.a. a computer.

Well, thanks for your time and I hope my letter serves some kind of purpose. See you all at H2K!

Anthrax

When things like this happen, you need to get names and witnesses. Unless you're leaving out some vital detail, your rights were severely violated. You cannot have such things confiscated by security guards in an airport. To have reading material questioned, especially on a domestic flight, is absolutely unacceptable. We hope that if this happens again to anyone, that they make a major fuss, even if it doesn't seem to be a big deal. Trust us, it is.

Dear 2600:

Someone ought to teach priceline.com a lesson. I recently purchased a plane ticket through priceline.com without realizing that I entered the wrong return date (damn clock on my computer was reset and I forgot to set it back to normal). Well, I got the ticket and then went about trying to change the return date back to the one I actually wanted. Damn bastards wouldn't let me, even though it was an honest mistake. I then went to Delta Airlines and tried convincing them - no such luck. So now I'm stuck spending 400 bucks for a 175 dollar ticket. Damn, I wish I could be a ninja.

SHemp5150

Dear 2600:

In yet another breach of freedom, corporate America has shut down another site with threats of legal action. You guys remember the "Dislectizer"? Funny little CGI program that would take someone's site and reword it as it would be written by Elmer Fudd or the Swedish Chef. They also did Redneck, Cockney, and Jive too! Pretty harmless and amusing, right? Not so, says corporate America... check out the notice on the site now at rinkworks.com/dialect/notice.shtml. Basically so many people have threatened the author with legal action it isn't worth his while to keep fighting them anymore. Absolutely-fucking-ridiculous! Where will it all end? When the "mega-corporation" owns everyone and everything do you think it will stop? Then what? Maybe we will have to beef up space exploration so we can start taking over alien cultures too.

KoDo

There is no misunderstanding here. The web has become a battleground between free speech and corporate interests. Never before have so many people been threatened. But we have many many individuals on our side from all over the world who have a chance to win the war as long as they don't back down. It's not going to be easy and it's not going to be pleasant. But if we let these powerful entities dictate how we express ourselves, we will have lost the most powerful voice we've ever had.

Dear 2600:

I enjoy the free speech and thought forum that your magazine provides for those of us who prefer to go against the conformist views of society. I have felt the need to write you regarding a bit of injustice that I have been subjected to. I have been working for a Fortune 500 IT services provider as a data recovery specialist at a Fortune 100 gas manufacturing corporation for the past 2.5 years. Now that I have accepted a job offer from a small, local ISP as a UNIX/web administrator, I can write without fearing for my job. Approximately 1.5 years ago, one of my primary duties, in addition to a host of other things, was programming of print servers for the gas corp's LAN. This was accomplished by telnetting into a VAX/VMS system from a Windoze desktop box, then using NCP to connect directly to the MAC address of the print server. Now, let's think about this for a moment. Whoever has this password can connect to *any* ethernet interface on the LAN as long as they know the MAC. Sexy, huh? Anyway, once inside the print server, I was supposed to set the IP numbers, hostname, turn off all the protocols except for TCP/IP, and run a queue test. Those in charge of the corporate "process" for doing this had instructed us to do it using four enable/disable commands, one for each protocol. The documentation for the print server revealed that, using a slightly different context, TCP/IP could be enabled and all other protocols disabled with *one* command. In the interest of efficiency, I took it upon myself to concatenate these four commands into one and use the shortcut from now on. About three or four months later, I received a telephone call from the head of Network Printing, in which he informed me that "just between us" several LAN printers were dropping off-line and they had suspected a hacker of causing the damage. He then asked me to read back the commands I used to configure print servers. At this point I recited my modified version of the syntax that I had been using from memory. "OK," he said. "We'll be in touch." A week later, I was told that the liaison between our company and the contract would like to speak with me. I walked into the meeting room and there sat my supervisor, the head of MIS Security, the head of the Help Desk, and the Network Printing Team. "What the fuck is going on?" I wondered. I was taken aback when I found out. They told me that I had deviated from the approved corporate process for configuring print servers and that, in my concatenating of these commands, I had caused servers to be dropped from the LAN at random. That was an obvious crock of shit to anyone who has a moderate amount of networking knowledge. I was then forced to go meet MIS Security for an official interrogation where I was watched while programming a server. When I entered the four commands into one, Security demanded to know where I learned these "unapproved commands." I explained that simple, logical shell knowledge was all it took to figure it out and that the end result was identical. I was stripped of my ID badge and parking pass and was told I would not be able to return to work until the issue had been investigated by the proper

authorities. During my suspension, I researched the issue at hand and found a document on the print server manufacturer's web site explaining that there was a bug in older firmware revisions of the card that a DHCP=1 flag would override a hard coded address after one server reboot. What was actually happening? The print queues would lock and in order to clear them, the local admin would reboot it. Upon rebooting the server, it would look for a DHCP address, not be able to get one, and then set the IP to 0.0.0.0, dropping it from the LAN. Returning to work ten days later, I presented this information to the proper authorities, only to be told that my future with the company "didn't look good." I was then told to write a kiss-ass letter to those involved in order to keep my job. I complied. After all, I had to pay my bills and didn't have any back-up plan. A week later, nothing happened to me, but the print team had released a formal memo updating their original instructions with both the concatenated commands and the DHCP=0 setting and, of course, taking full credit for the fix. I just wanted to share yet another example of how Corporate America continues to persecute us for individual thought, benefit from our knowledge, and then take the credit for it.

diss0nance

Starting a New Meeting

Dear *2600*:

I am an avid reader of your magazine and enjoy it very much. But I feel I am missing out on something by not being able to attend any local meetings because, well, there aren't any. I live in the small, boring state of Delaware. Where can I find other interested people in my area who would be interested in starting meetings? I want to help spread knowledge so that our society in Delaware will be more educated about hacking.

Nu1.1. val.ue

We're certain there are more people in your area who share your interests. We suggest finding a place that's easy to get to and in a fairly populated area. Check the guidelines on our web site and get the word out however you can. It can take several months to build a meeting so don't give up. Here's proof that there are people around you who would go.

Dear *2600*:

I would just like to say that I think the MPAA and NBC are a bunch of money hungry assholes. I have printed out and posted over 200 flyers all over Wilmington, Middletown, and a couple of other places in Delaware. I went into video stores and gave people copies. I am just trying to raise consciousness about all this crap.

neurophilter

Praise

Dear *2600*:

My hats off to *2600* - the only online hacker resource that has so much as mentioned the week long protests against the IMF and World Bank in Washington DC, April 8-17. It's sad that the world of freedom seekers is so divided and most hackers see only software and hardware and not world issues. After reading other hacker and "geek" interest web sites and online publications, one would have no idea that there was a revolution in the making.

Once again, job well done. Keep up the good work.

Dave
NYC

You don't have to be a weatherman to know which way the wind is blowing.

Dear *2600*:

I'm a new reader of *2600*, my first issue being the "1999-1900" one. The magazine seems to attract a surprising range of readers of all levels of intelligence. Mixed in with the great letters about recently found exploits or information on which military software package-of-the-week has absolutely no security, you've got the geniuses who want you to help them vandalize their school's web site or who just want to steal something from Borders. In dealing with all this, you excel at calmly reading their messages and adding a bit more information where needed or politely showing them exactly how stupid they really are (not that they're likely to notice the sarcasm in the response).

Anyway, I just read the pair of interviews cnn.com has about hacking (located at www.cnn.com/TECH/specials/hackers/qandas/). Great stuff. While you replied to the questions with honesty, patience, and information, the good doctor comes off as a corporate stooge. Where your responses are well thought out and straightforward, we get Dr. Palmer calling hacking a felony, while immediately proceeding to discuss all the "ethical hacking" his organization engages in.

First of all, I'd like to see the law that makes hacking a felony, and second, I'd like to know how adding the word "ethical" makes something less felonious. While these interviews (when the replies are included verbatim and not edited for space) almost *always* show *2600* and the hacking community in a good light, any time such an interview is paired with the corporate line about hacking, the suits come out as intolerant incompetents spouting menacing sounding technobubble. Let's see more interviews like that!

By the way, I work at an independent K-12 school that is thankfully run by tolerant, thinking individuals. So as long as I'm here, my copies of *2600* will always be sitting out on my desk for the students to read. Just so people don't get the idea that every school is an oppressive tool of the state.

Da Clyde

Dear *2600*:

I am writing to congratulate you for publishing one of the most incredible issues to date, namely the Spring 2000 issue. Each article was interesting, well written and, most importantly, practically informative (i.e., "Securing Web Sites with ASP"). The Kevin Mitnick article was awesome. The "How to Stay a Sysadmin" should be required reading for the entire IS community. The article was so true - I have forwarded it to friends and coworkers. Every time I buy an issue of *2600* I never know what to expect. This time you exceeded my already high expectations. Consider me from this point forward a subscriber. My check is in the mail. Keep up the good work and thanks for keeping the world safe from unjust corporate/government oppression. An informed citizen is a better citizen.

3_trinity_3

ANAC Numbers

Dear *2600*:

In issue 17.1 someone named casey wrote in stating that 958 will read back the number you're calling from. It doesn't work over here in Thousand Oaks, California. The magic number here is 114 (like backwards information). Just thought you'd like to know that 958 doesn't work everywhere.

Goop

Dear *2600*:

I saw in the Spring 2000 issue that you guys mentioned that you can dial 958 or 9580 to have the number you are calling from read back to you. In my area (McLean, VA) those numbers do nothing. Instead we dial 811.

Best of luck dealing with the MPAA. You guys should file a class action suit against them for violation of the Sherman Antitrust Act. (History class actually being useful! I never thought I'd see the day!)

PaleronD

Media Misrepresentation

Dear *2600*:

Last night on the radio and more in depth today in the *New York Times*, there was news of Mafiaboy, the kid who allegedly launched the DoS attacks on CNN, being caught. Although I think what he did was completely juvenile and stupid, on NPR they were talking about how "security experts" were saying that Mafiaboy caused around $60 million in damage. Reminds me of the Kevin Mitnick saga! The CNN site was down for two hours, people.

phil

And a recent e-mail "virus" was said to have caused over $10 billion in damage! The numbers are pretty obviously nonsensical. It's not unlikely that most of whatever else these people are saying is as well.

The Staples Threat

Dear *2600*:

In issue 17.1, on pages 35 and 36, you published a letter from Jack A. VanWoerkom. I would like to commend you on your smart, cheeky reply. I am gratified to know that *2600* stands by its convictions and will not disclose the identity of any of its sources. I am wondering if Staples kept their promise of legal action. Though important to stand your ground on any such issue, it undoubtedly comes at a terrible time, due to your current involvement with the MPAA lawsuit. I would like to express my support for *2600*. I hope we end this trial by shaking up corporate America, and opening the public's eyes to such corruption. Education is the key.

Cielo

We expected an increase in attacks on us because of a perceived weakened state. But this is nothing compared to what will happen if we don't resist each and every time we're pushed.

Dear *2600*:

This is in response to the letter from "Jack A. VanWoerkom, Senior Vice President, General Counsel, Staples" in 17:1 regarding my article on Staples in the preceding issue.

Firstly, I haven't heard a title like that since the book *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw by The Man Who Did It* came out.

Secondly, Jack (may I call you Jack?), you "demanded" that *2600* identify me, under threat of legal action. Well, I'm sorry to say that *2600* doesn't know who I am and therefore cannot tell you, even if they wanted/were forced to.

Thirdly, you repeatedly mentioned "trade secrets" and "proprietary information" in your letter. I doubt you are saying that the fact that EAS (Electronic Article Surveillance for you home players) stickers can be removed from products is "proprietary information." And since most of the other information in the article can be observed with a minimum of effort by a determined observer, the only things you could be referring to as "trade secrets" are your passwords. In this regard, I have two points: First, aren't you glad it was someone like me who found out your passwords? I mean, at least I notified you (indirectly, granted) of the problem. It *could* have been someone with a malicious streak who could have wiped out all your files, or, worse yet, screwed with your system so cleverly and subtly that you still wouldn't know, years (and tens of thousands of dollars of losses) later. Now, because of me, you are warned. And hopefully, you will take precautions to prevent unauthorized access to your store's computers. You're welcome. My second point is in regard to your passwords themselves. While "01BSdaIWH.9" is a reasonable password for an Administrator account, it really should have some more non-alphanumeric characters in it to make it tougher to brute-force. Having a password be only four characters makes it *extremely* easy to brute-force. Especially when the words are obvious ("SELL") or taken straight from corporate brainwashing literature ("CARE"). Using the stock symbol ("SPLS") is just plain dumb, as is using the store's name followed by a simple digit series ("Staples1234"), or the login name backwards ("ecivreSselpatS").

Fourthly, I have some suggestions for you on how to beef up security at the store level. Besides changing your passwords to something a *little* less obvious, I would suggest that you have floppy drive locks installed on all the computers, includ-

ing the ribbon computer and those in the manager's offices. You should change the default password for your phone systems as well and cease using "Fred Klein" to rally the troops (perhaps you could switch to "Jack VanWoerkem"?). Now, I normally charge $40 an hour for simple security audits, but you can have this one free... this time.

Finally, since you seem to dislike knowing about any security problems Staples may have, I won't say a word about those dial-ups at the Home Office, the fact you still use default passwords for your AS400 system, or anything about your web site.

Maverick212

Y2K

Dear *2600*:

I'm sitting here looking over the 17:1 issue of *2600* and was noticing the many "year 2000" bugs that happened with the mag. I would just like to say it was a nifty little bug that hit.

MoJo

Sure, get a little enjoyment out of our pain and frustration. What a nightmare. Fortunately, we seem to have managed to get the bugs ironed out once and for all. Thank you CERT.

True Security

Dear *2600*:

I was recently on the United States Postal Service web site looking up a zip code when I saw something that I couldn't help laughing at. They have this online service called USPS eBillPay, which can be used to pay postage and other charges online. On the main page, there is a little logo with text that reads: "USPS eBillPay: As secure as your mailbox." Now, how many people really have "secure" mailboxes? I clicked on it anyway and read more about it on the next page. They go on and make another statement about security: "Secure? Of course! It's the United States Postal Service!"

pulse

Considering most mailboxes don't even have locks of any sort, that is a rather frightening claim.

Listening In

Dear *2600*:

I just had to finally write and speak my piece. In 16:4 Black Axe wrote an article "An Intro to Paging Networks and POCSAG/FLEX Interception." First I must thank Black Axe for all the hours of pure fun I have had intercepting paging transmissions. The world between radio technology and computer technology is growing ever closer. Anyway, I thought I would share this little piece of the paging airwaves I picked up one night: "Msg:Computer crime 'in progress' diverting c c #s. Call me @ 894-5272. ADP#9" Can you believe it? "Computer crime in progress." I actually called the number and found out it belongs to an e-commerce business. The guy answered, but I didn't feel like social engineering that night so I hung up. It occurred at about 9:12 P.M. Thanks again for all the fun!

zzflop

Female Hackers

Dear *2600*:

I've noticed that females usually don't send letters to *2600*. This is because, like most of the computer industry, girls don't usually hack or aren't extremely knowledgeable about computers. I myself am and many people think this is odd. I do not brag about what I do, but anyone who knows I'm interested in computers thinks it's strange. For example, I'm the only female in my computer maintenance class in school. The Internet is a great place for women to hide their identities and get ahead. Many hide behind handles and such and guys treat them just like one of the guys. I don't know. Do guys like females who hack? Are they well respected in the hacker community? So far, I've only had a few problems with my sex in the community. I just wanted to know other female hackers' opinions on the subject. I think that the Internet is great, because most of the people you talk to just assume you're a guy and they have no problem chatting with you. Just wanted to know if female hackers out there *are* getting the same respect as me.

MiSsReSS DiVA(aka-Beul)

We find that you're treated with more respect if you don't make an issue of these things to people who don't know you at all. Your ideas and words are what people should judge you by and when you start to define yourself in your name (using words like "boy" or "girl") it's hardly surprising when people treat you differently. Some people want this but for those who wish to experience the amazing anonymity of the net, leave the personal descriptions for later.

Desperate

Dear *2600*:

I am really desperate to hack a site and change their stuff. I have been looking at your site forever. I need to hack. *I am desperate.* Please help me.

From a Wanna be Hacker

Yes folks, this is the threat to the nation's infrastructure you've heard so much about.

The Verizon Threat

Dear *2600*:

I just read your web article on the Verizon problem concerning domain registration, so I registered VerizonSucksDick.com about five minutes ago just to see what happens.

majickmutex

Last we checked, those domains are going fast. Between the 706 names that Verizon already registered and all of the ones that people are registering now as a protest against their threats, the people benefiting the most are the domain registrars.

A STUDENT'S PRIVACY SECURITY SURVEY

by Pip Macki

This is a survey of the security of private student information on college campuses. The particulars in this case were collected at the California State University at Chico. Rather than undergoing a comprehensive security audit, these are only the vulnerabilities that are casually apparent. Most of these issues have been observed by students during the regular course of registering for classes, checking grades, etc. The scope of this survey only includes network and administrative policy, and network security. While there may be machines on these networks running services that are vulnerable to attack, all of the issues raised in this survey exist independent of any exploitable services.

Numerous university databases contain personal student information. Most of these databases receive information at one point or another from the mainframe (CHIMVS). This machine hosts the Student Information System (SIS+), a database that contains, among other things, information on the enrollment status, grades, test results, and immunization records for all Chico State students since the system was put into place.

CHIMVS is running OS/390 with a front-end called Telescreen. Telescreen has C2 certification, but only when it is properly configured. University administrative staff connect directly to Telescreen via a TN3270 client. This access method is used for everything from reserving a room to changing a student's enrollment status. Not only does TN3270 use plain-text authentication, there are no apparent TCP wrappers implemented, no firewalls (or a non-configured firewall), and many unsecured machines on the same LAN which still contains numerous non-switching hubs. Essentially, traffic is wide open to the entire world, with little if any distinction between trusted and non-trusted networks.

It would be trivial to install SSH or tunnel TN3270 through an encrypted layer. Such basic steps would eliminate an intruder's ability to pilfer passwords from a compromised machine from which users do not directly access CHIMVS. Packet sniffing would still be a threat even if the server were separated from the Internet and student networks. There are currently no secure means available for accessing CHIMVS. All users are forced to login without encryption. Physical access to Ethernet cables is also not difficult for a determined intruder to obtain.

Given the current setup, all IP addresses are allowed to connect to CHIMVS and potentially login. CHIMVS' direct and unfiltered connection to the Internet greatly increases the number of people who are able to access SIS+ without any possible legitimate reason for having access.

Only trusted computers on the correct interface should be able to connect to CHIMVS. However these computers (and their users) aren't worthy of trust themselves. Currently these workstations are just as exposed as CHIMVS, but are far more vulnerable to attack because they are also being used to access the world wide web and retrieve e-mail while running notoriously insecure operating systems such as Microsoft Windows 95 and NT. Some of the Windows workstations have a virus scanner like Network Associate's V-Shield installed and prevent the long-term installation of new programs by re-mastering the hard drive from a central file server after each reboot. Should the central file server be compromised, the results could be devastating. All it takes is one workstation infected with a trojan horse like BackOrifice 2000 (BO2K) to permit an intruder to sniff the net-

work traffic for passwords and student information, log users' keystrokes as they enter their login and password, and use the trusted machine as a proxy to connect to CHIMVS. Since BO2K is open source, it can easily be modified and recompiled to slip pass conventional virus scanners.

Upon submitting forms to the Admissions and Records Department, students have been known to have a clear view of the terminal's screen. One such screen displayed a TN3270 client (showing the record of the previous student) and a minimized session of the Microsoft Outlook e-mail client with the user's e-mail address visible. There is a long list of methods for delivering a trojan, and programs like Microsoft Outlook and Internet Explorer make it very easy for a user to unwittingly execute hostile code simply by viewing a document or going to a web site. While the monitors can be repositioned so that they are no longer visible to shoulder surfing students, finding out a user's e-mail address is as easy as calling on the phone and asking their name. A complete and searchable directory of users' e-mail addresses, names, phone numbers, and departments is accessible from the Chico State web page at www.csuchico.edu/cgi-bin/address. Department secretaries and other staff are still susceptible to shoulder surfing and social engineering.

Any machine containing sensitive information should have no Internet connection whatsoever - it is an unnecessary risk and of questionable value. Failing that, a properly configured firewall is essential. Setup of all incoming connections should be denied, with outgoing connections limited to pre-approved TCP ports, like 80 for http, etc.

Onsite Mischief

There is still the issue of sharing information with other databases. Campus Computing and the College of ECT maintain a user database that uses Student ID (SID) numbers copied from SIS+ for tracking and identifying e-mail and shell accounts. Student ID cards contain a globally unique identifier (GUID) that is a different number than the SID (which in the vast majority of cases are Social Security Numbers). The Student ID card system is used as positive identification for students, faculty, and staff. Their magstripes and barcodes contain the non-SID GUID and are used as a means of authentication for creating e-mail accounts and to toll meals from dining hall meal plans. This database is maintained on a system known as ICAM which ties Student ID card numbers to SIDs (obtained from SIS+), along with a photograph of the person and meal information. When a meal is used, the card is swiped at a point of sale terminal connected to ICAM or some intermediary computer via a serial port. An observant student would notice a serial cable going from the magstripe reader into an exposed and accessible punch-down junction box in the basement rec room. It is a simple matter of plugging the serial cable into one serial port of a laptop, and the other serial port into the junction box and running a sniffer to pilfer Student ID card numbers, which can then be used to rewrite a magstripe in order to steal meals or create e-mail accounts as someone else. The ICAM system itself fails in many of the same ways as CHIMVS because of its lack of isolation and protection.

The College of ECT breaches students' privacy by associating their full name, obtained from SIS+, with their system user name, and publishing it in a public directory. It is impossible for a student to modify this entry, as it exists independently of the system password file. The e-mail account system currently uses SIDs to keep track of user accounts. It regularly checks SIS+ for the major and enrollment status of each account holder to verify which machine their account should be on. If SIS+ used the Student ID card number as the SID, it would eliminate the need to cross-reference the two GUIDs.

It is possible to obtain a non-SSN SID. However, if one first registers under their SSN and then changes to a fictitious number, it is still cross-referenced with the original SSN and there is no system in place to enforce the change in all of the various databases - causing much confusion and generally breaking things. It is also possible for a student to change the PIN (set to their date of birth by default) with which they access their accounts via TRACS to register for classes and to check account information via the Student Personal Information web page. The combination of SSN and DOB as a means of authentication are very poor choices. They are easily obtained and guessed (respectively) pieces of personal information. CNS, the Communications Network Services (www.csuchico.edu/csrv/cns), which provides telephone service for students living on and off campus uses social security numbers to identify students' accounts. They have been known to hand people their phone bill (containing full account information) without checking a photo ID - only their phone number. Once a person's SID has been discovered, it is a simple task to automate sequential dialing (wardialing) of TRACS (www.csuchico.edu/schedule/tracs_book) until the right PIN is entered. Alternatively, one could theoretically write a program to sequentially enter PINs to the https://www-sis2.csuchico.edu/SalvoC/mvstart2.htm web page login. Limited testing did not indicate a login retry limit per IP address.

Like a traditional dictionary attack, the pool of possibly PINs can be narrowed significantly. First, by limiting it only to valid dates and a range of years consistent with the possible ages of the target. In the rare case of someone actually having a non-DOB PIN, the chances are it is still six digits and one can work down from that. The Student Personal Information web page's CGI has numerous potential vulnerabilities, most of which were not tested conclusively, not the least of which include buffer overflows and man-in-the-middle attacks. The login page for the CGI is displayed in a JavaScript pop-up window and encrypted via SSL. Various measures are taken to try to protect users' sessions, the login and PIN must be reentered each time a new request is made, and sessions timeout in a short amount of time. But despite using SSL, the mistake is made of transmitting the login and PIN via the GET method of an html form tag, rather than the POST method. Thus the login and PIN become part of the URL the browser goes to, and it is saved in the browser's history file and any bookmarks that are made of the page. Bugs present in both Internet Explorer and Netscape allow previously accessed URLs to be erroneously reported as a referring URL to subsequently visited sites - further increasing potential exposure. Checking the history files of public lab computers around grade reporting time could prove quite fruitful.

After taking the training course for using SIS+, it is not uncommon for users to write their password on the inside cover of their user manual. Asking to borrow a department secretary's manual is one very easy technique for gaining access - the Chico State web page (www.csuchico.edu/tlp/resources/oncampus/master/rmavailres.html) even offers this friendly advice for those seeking to reserve a room. *"Most department secretaries have an account and password to access SIS+. Below is a list of steps to access SIS+ for anyone who has a computer, a network connection, and a SIS+ account and password...."*

In a red-tape filled bureaucracy like a university, sometimes the easiest way to analyze security is from the outside. However, to perform a truly comprehensive security audit, proprietary knowledge of the University's database management would be needed, along with a whole lot of permission.

FREEDOM DOWNTIME

MARKETPLACE

Happenings

H2K - HOPE 2000 will be taking place on July 14, 15, and 16, 2000 in New York City at the Hotel Pennsylvania (the site of the first HOPE Conference in 1994). This time we have two floors and enough room to do whatever we want. If you haven't waited too long to read this, there may still be time to make it! Reserve your room at the hotel by calling (212) 736-5000 (worldwide) or toll free (dial PEnnsylvania 6-5000). Mention that you're with the H2K conference to get the discounted rate. Unlike previous HOPE conferences, we will be running this one around the clock beginning on Friday morning and ending on Sunday night. We will have two tracks of speakers plus an open mike as well as music, films, and a presentation of all sorts. Catch the world premiere of the 2000 documentary "Freedom Downtime." hear keynote speaker Jello Biafra, participate in our mock trial against the MPAA, stay an extra day for the REAL trial on Monday the 17th at the Federal Courthouse downtown. Meet hackers from around the world as we share info on all of the latest developments. A full program will be posted on our website. Registration for H2K is $40 and includes admission to all events throughout the three days. Advance registration is closed - you now can only pay at the door. Continue to check www.h2k.net for updates.

DEF CON 8 is July 28th to the 30th in Las Vegas. Wacky hackers descend on Las Vegas for the eighth annual computer underground convention. Last year over 3,000 people showed up to party, exchange information and ideas, and hack on the local network. This year we have the entire Alexis Park resort to ourselves, which means almost double the space! This means more speeches, more demonstrations, and more things to do. There will be the fantasy net connection. Capture the Flag network contest with new rules and goals. The Spot the Fed Contest, and the social engineering contest to name a few. There will be live bands and an even larger 24 hour rave area, a vendor area where people can sell shirts, tools, and other goodies. This year the speeches will be separated into different tracks, from "newbie" talks designed to introduce new hackers into different areas of interest to "Uber Haxor" for those people looking to refine their skills or get the latest tech info. Any of this stuff get your attention? Even if it doesn't you can still hang out by the pools and watch the conference through the hotel TV system! Check out www.defcon.org for the latest planning information and speakers, or for previous year's speeches. Email The Dark Tangent (dtangent@defcon.org) for more information.

For Sale

HACKERS WORLD. 650 MB of hacking files $15. Anarchy Cookbook 2000 $20. Virus 2000 (351 pages of computer viruses) $10. Make Money Fast (250 ways to make money on the Internet) $5. Phone Bug (no bugs, the real device) $10, cell phone pickup device (just aim at the phone and hit the button and it picks up the call with little static) $20 for plans and $30 for the device. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd. CD-ROM PDF/GIF version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full-sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items made of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com.

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

HTTP://PACKOS.COM since 1996. Lockpicks, auto entry sets, confidential trade publications, survival tools, an exciting line of affordable switchblades, powerful air rifles and pistols, and a complete line of super-realistic Airsoft guns. Danger: do not brandish these guns in public; you may be arrested/shot. We guarantee what we sell UN-CONDITIONALLY for 30 days, in addition to factory warranties, and will beat the competition's prices hands down! No "toy store" or "Y2K" hype here, you won't believe it! Visit us to post messages to our discussion board, add your email to our mailing list, or place an order with our easy-to-use catalog! We can ship internationally, and will only sell to qualified customers. U.S. customer can now pay with VISA/MC.

PLAY MP3S IN YOUR CAR OR HOME! Mojuke unit plays mp3 cd, cdr, and dvd disks. Can be mounted in car, home, or even inside a free drive bay of a PC. It can be trunk mounted in a car or placed under the dash. The unit is self contained, pre-assembled, and it includes a wireless remote. For more information, visit: http://www.mp3carplayer.com/2600 or e-mail 2600@mp3carplayer.com. Sign up for our affiliate program and earn some cash. Resellers needed. $25 from every 2600 sale will go to the Kevin Mitnick fund. We will ship anywhere that we can.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of Infiltration, the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $6 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - at: http://users.aol.com/caravela96 - and a novel "Rage of the Bear" by Burt Byfield about a 15-year-old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QH39, 134 Goodburlet Road, Henrietta, NY 14467.

INFORMATION IS POWER! After years of being in the scene we've put together a publicly accessible site for people to talk about a wide variety of hacking genres. In addition, we have obtained tools for our own private news center for information and articles about current computing happenings worldwide. You can find all this, and more, on our site at: www.wattnesscorp.com.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers Encyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $15 includes shipping (TAP logo in black on a white 100% cotton shirt). As seen at Beyond Hope.

Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 40A Weis Rd., Albany, NY 12208.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

Help Wanted

POLITICAL PRISONER has non-profit organization, developed his own primitive web pages to foster political support for his release, but has no one to post his work on the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwainClemency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMar, Director, Sean Swain Clemency Campaign, P.O. Box 57142, Des Moines, Iowa 50317. (515) 265-2308.

LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-2686 for further details.

NEED HELP ON CREDIT REPORT, ex wife screwed me. Please reply to: I4NI, 5128 W.F.M. 1960, PMB#215, Houston, TX 77069. "Michael"

I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chao, PO Box 375, Middle Village, NY 11379.

NEED HELP WITH CREDIT REPORT. Please respond to R. Mandel, 433 Kingston Ave., P.O. Box 69, Brooklyn, NY 11225.

HELP TO FIND TROJAN HORSE PROGRAM. Understand there is a Trojan Horse program which may be added as an attachment to an e-mail (which appears innocuous when viewed or read) but which will execute and record any password used by the recipient and then send it by e-mail to an outside recipient. Further, that if the outside recipient doesn't receive it for any reason, the e-mail message with password(s) will not bounce back to the sender. Also, there is another Trojan Horse program which, after it installs itself in the UNIX-based ISP of the target, will mail out copies of all incoming/outgoing to an outside recipient without the target being aware of it. Can anyone help with complete information, details, and programs? brynab@usa.net

I NEED TO OBTAIN credit report information on others from time to time with little or no cost. Can someone help? testtest@usa.net

NEED HELP FINDING AND USING WAREZ SITES. I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. E-mail netvampire@iname.com for list or details.

Wanted

MINIATURE PEN-MICROPHONE that is very sensitive and transmits at least 300 feet to an FM radio. Need the name/address of manufacturer(s) (and prices if available). Reply to bin/bd@usa.net.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13893228. I want the ORIGINAL copies only.

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1590, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

Services

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, at (334) 265-8602 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a samurai warrior committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 956-5591 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site. Your feedback is welcome at oth@2600.com.

THE FAMILY, a close-knitted anarchy social group has formed for hackers, phreakers, and computer nerds. Join with your kind in furtherance of independent ideology, financial freedom, and prosperity. Master the possibility of collective thought and association with members of your own mindset. For further enlightenment as to the lifestyle of the family, break the old mold, dare to explore, contact Purcell Bronson, Drawer K, Dallas, PA 18612.

Personal

I AM A FAIRLY INTELLIGENT PERSON with potential to be a computer geek looking for someone to give me one-on-one lessons in areas necessary to be a hacker by way of correspondence. I am presently being held captive by the Texas prison system and I have approximately 2 years before I am released and I want to familiarize myself with the basics and fundamentals of hacking during this period. Interested people contact me at: T. EDWARD JONES, No. 510071, HC 67, Box 115, Kenedy, Texas 78119, U.S.A.

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be viewed within the "Free Burma Coalition" web site. Thanking 2600 staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: www.brazilboycott.org

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/15/00.

[illegible]

DON'T BE SILENCED

The lawsuit against us by the Motion Picture Association of America continues with our trial scheduled for the day after the H2K conference!

You can show your support for 2600 and the other defendants in the MPAA case by sporting our stylish anti-MPAA t-shirt. The front looks a lot like the cover to our Spring 2000 issue while the back has the above scary caricature of MPAA chief Jack Valenti.

The shirts are $25 each, the proceeds of which go to the defense fund. In addition, we have "Stop the MPAA" bumper stickers (10 for $10) and "Stop the MPAA" buttons (3 for $10). Please show your support and help send a message that this affront to all of our rights won't be tolerated.

You can order all of these items plus our regular stuff through our online store at www.2600.com or by writing to us at:

2600
PO Box 752
Middle Island, NY 11953
U.S.A.